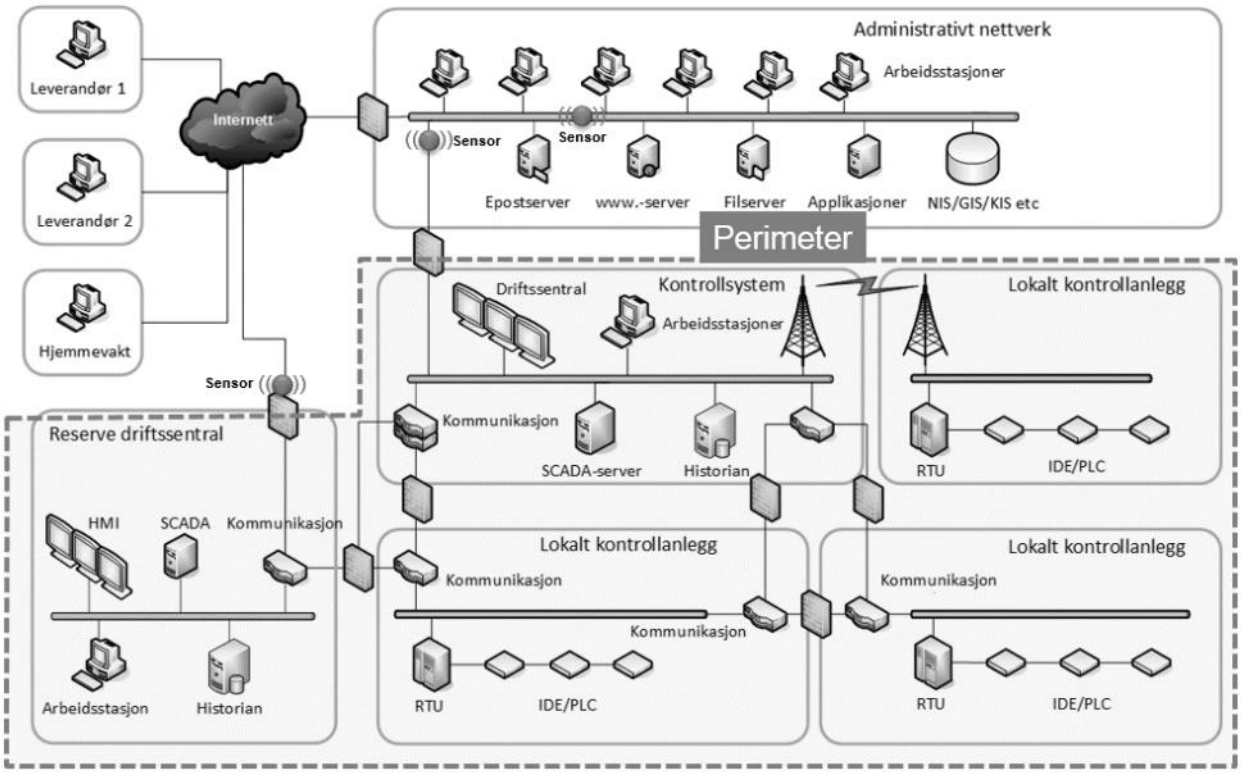
Innhold

7. Beskyttelse av driftskontrollsystem

Driftskontrollsystem er definert i § 7-1 i denne forskriften. I følge § 7-1 omfatter driftskontrollsystemer driftssentraler, utstyr, nettverk, datarom, sambandsanlegg og øvrige anlegg og rom, systemer og komponenter som ivaretar driftskontrollfunksjoner. Denne definisjonen er vid. Når enkelte krav er rettet mot det tekniske kontrollsystemet er dette kommentert spesielt under hver paragraf.

Driftskontrollsystemer er avgjørende for situasjonsforståelsen, effektiv drift, håndtering av ekstraordinære situasjoner og rask og trygg gjenoppretting av feil og annen skade på system og infrastruktur. Driftskontrollsystemet må fungere og gi korrekt informasjon selv ved langvarige og ekstraordinære hendelser. Dersom driftskontrollsystemet svikter, må virksomheten ha beredskap og planer for alternativ drift.



Figur 1 Driftskontrollsystem og administrativt nettverk. Alt innenfor stiplet linje regnes som driftskontrollsystem.

Kapittel 7 setter krav til sikring av driftskontrollssystemet mot en rekke farer og trusler. §§ 7-14 og 7-15 i denne forskrift oppstiller tilleggskrav til virksomheter med driftskontrollsystemer i klasse 2 og 3.

Driftskontrollsystemer styrer anlegg i ulike klasser. I driftskontrollsystemer skal elektronisk/digital kommunikasjon og datautveksling sikres i henhold til driftskontrollsystemets klasse, mens fysisk sikring skal gjøres i henhold til det fysiske anleggets klasse (se forskriftens kapittel 5 med vedlegg). Fysisk sikring av rom som brukes for driftskontrollsystemet i et anlegg, følger driftskontrollsystemets klasse hvis denne er høyere enn anleggets klasse. Driftssentral og datarom i uklassifiserte bygninger sikres fysisk i henhold til driftskontrollsystemets klasse.

7.1 Generell plikt til å beskytte driftskontrollsystemet

§

§ 7-1. ***Generell plikt til å beskytte driftskontrollsystemet***

Virksomheter med driftskontrollsystem skal sørge for at disse til enhver tid virker etter sin hensikt og skal beskytte driftskontrollsystemet mot alle typer uønskede hendelser.

Driftskontrollsystemer omfatter driftssentraler, utstyr, nettverk, datarom, sambandsanlegg og øvrige anlegg og rom, systemer og komponenter som ivaretar driftskontrollfunksjoner. Med anlegg forstås også tilhørende bygningstekniske konstruksjoner for driftskontrollfunksjoner.

Driftskontrollfunksjoner er alle organisatoriske, administrative og tekniske tiltak for å overvåke, styre og beskytte anlegg i kraftforsyningen.

Det tillates ikke at eksterne leverandører som ikke er KBO-enhet, utfører driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg.

Ordforklaring

Ord	Forklaring
Driftssentral	Rom i bygning med driftskontrollsystem som ivaretar driftskontrollfunksjoner og består av skjerm, tastatur, server, datanettverk, UPC og annen nødstrøm, samt klimaanlegg. I tillegg inngår servere, rutere, UPC og annen nødstrøm, samt klimaanlegg i tilhørende datarom og sambandsrom.
Utstyr	Tekniske komponenter og instrumenter, herunder for eksempel dataskjermer, servere, tastatur, PLC, vern, brytere, svitsjer, rutere, sensorer mm og hjelpemateriell.
Komponent	Del av et system, instrumentdel
Samband	Etablerte forbindelser for overføring av kommandoer, måle- og tilstandsverdier, meldinger, samtaler, bilder, skriv, kart eller andre dokumenter og data mellom to eller flere punkter.

Hvordan oppfylle kravet

§ 7-1 pålegger en generell plikt til å sikre driftskontrollsystemet. Bestemmelsen krever at driftskontrollsystemet skal virke og respondere som forventet på måleverdier og meldinger fra anlegg som overvåkes og på kommandoer gitt av operatører på driftssentralen eller lokalkontrollanlegget. Det er kun godkjente brukere som skal starte, endre eller stoppe kommandoer i systemet. Virksomheten skal beskytte driftskontrollsystemet mot alle typer uønskede hendelser, se § 2-3 som setter krav til risikovurdering. Hendelser som inngår i risikovurderingen, bør samsvare med hendelsene som legges til grunn for beskyttelsen av driftskontrollsystemet.

Sikkerhetsstyring og tilhørende dokumentasjon skal inngå som en del av virksomhetens internkontrollsystem (§ 2-10).

Det er kun KBO-enheter som får lov til å overvåke og styre nett- og produksjonsanlegg som er underlagt denne forskriften. Driftssentralsamarbeid mellom ulike KBO enheter er tillatt. Andre enn KBO-enheter kan ikke overvåke nettet med bryterinnstillinger og utføre kobling. Det er tillatt at et vaktselskap overvåker og beskytter et kraftforsyningsanlegg ved å ha vakter på stedet. Tilsvarende er det tillatt å benytte programvare for å overvåke og beskytte driftskontrollsystemet mot digitale trusler.

NVE skiller mellom fysisk og logisk sikring. Den fysiske sikringen av driftskontrollsystemet skal være tilpasset det stedet anlegget eller bygningen befinner seg, og skaden som kan skje dersom noen utfører for eksempel hærverk eller sabotasje på stedet. Den logiske sikringen skal være iht. den av de tilkoblede anleggene med høyest klassifisering. Anleggene skal beskyttes for påvirkning fra punkter på sambandsveien, samt skal beskyttes for påvirkning fra andre lokasjoner. Alle selskap må foreta en risikovurdering av sambandsstrukturen slik at driftskontrollsystemet ikke skal kunne påvirkes fra anlegg av lavere klassifisering, se også § 2-3 som setter krav til risikovurdering.

Fysisk sikring

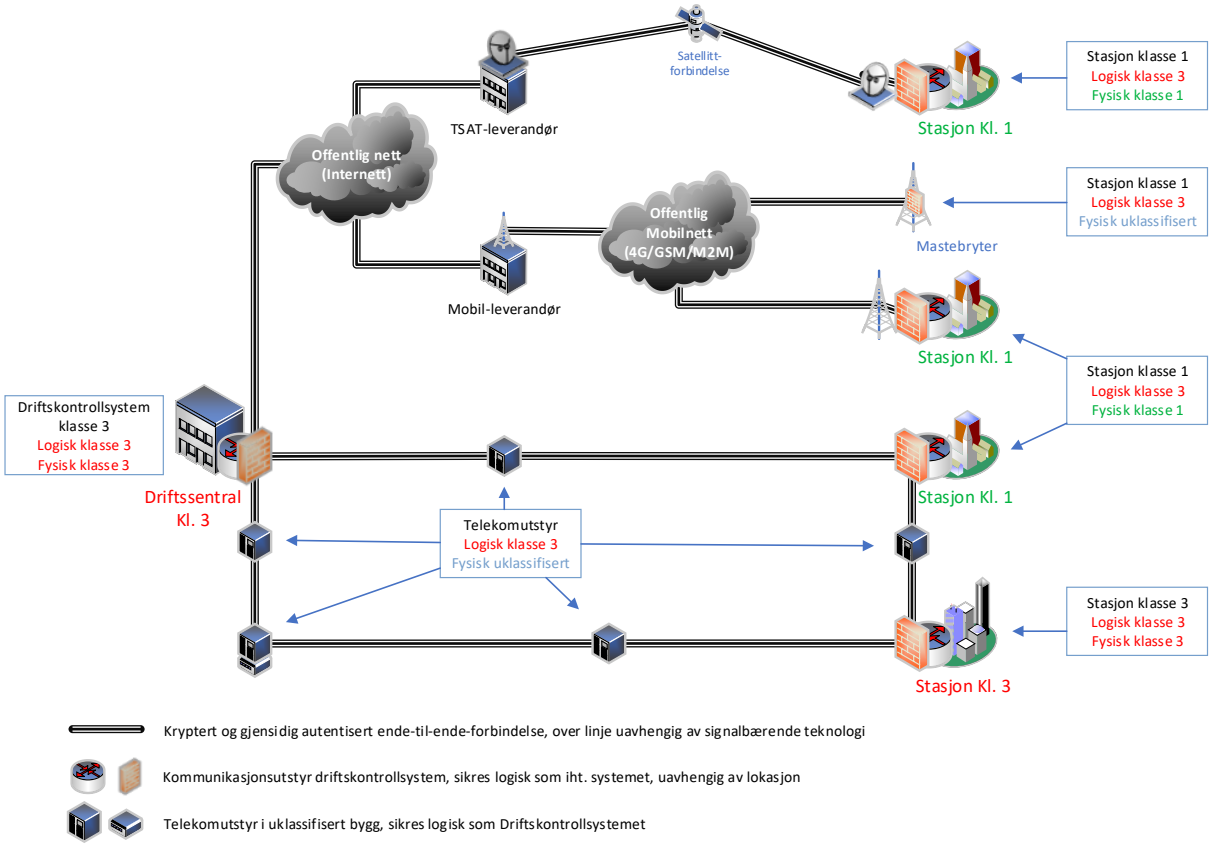
Sambandsanlegg og lokalkontrollanlegg går som regel gjennom skap via rekkeklemmer til avgrening og fordeling, til forsterkere, antenner og annet. Slike skap er det ikke mulig å sikre etter driftskontrollsystemets klasse, og blir derfor sårbare angrepspunkt. I en klassifisert stasjon står skapene innenfor et gjerde eller inne i en bygning og er sikret med områdesikringen, skallsikringen eller sonesikringen. Utenfor klassifiserte anlegg har slike skap ingen sikring utover styrke og lås. Ved valg av skap, må det kunne dokumenteres den vurderingen som er gjort angående skapets styrke, kvalitet på hengsler og lås, korrosjonsbeskyttelse og beskyttelse mot vann og fukt.

Når signaler og målinger går i et redundant system, er ikke ødeleggelse av komponentene i et skap tilstrekkelig til å forhindre funksjonene i systemet. Uten redundans er ikke dette tilfelle. For sambandsanlegg viser vi til kravene i vedlegg 1, 2 og 3 til kapittel 5, punkt 1.2.2, 2.4.2 og 3.4.2.

Logisk sikring

Det skal alltid være ende-til-ende-kryptering i samband fra sentral til stasjoner, og mellom stasjoner, dersom kommunikasjon går over uklassifiserte eller lavere klassifiserte komponenter/linjer. Dette kan realiseres ved å sette ut utstyr foran driftsutstyret på stasjon/sentral eller ved direkte ende-til-ende-kryptering mellom SCADA og RTU. I tillegg må det iverksettes beskyttelsesmekanismer, som brannmur, portautentisering, osv. på driftssentral/stasjoner for å beskytte mot påvirkning fra en mulig kompromittert lokasjon. På denne måten vil en angriper ikke kunne få innsyn eller tilgang til andre komponenter dersom sambandet blir kompromittert, og vil ikke kunne bevege seg videre fra en stasjon som er kompromittert. Dette betyr at det verste som kan skje om noen tar seg inn til utstyret er at forbindelsen blir brutt. Dette vil man være beskyttet mot med redundante sambandsveier.

Denne type sikring skal gjelde uansett transmisjonsmedier, også om dette går via f.eks. mobilnett.



Maler

Standarder

ISO/IEC TR 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry

IEC 62443 Industrial Automation and Control Systems Security

NERC-CIP (North American Electric Reliability Corporation critical infrastructure protection)

NIST 800-82 Guide to Industrial Control Systems (ICS) Security

Veiledere

NSMs Grunnprinsipper for sikkerhetsstyring

Guide to Increased Security in Industrial Control Systems, MSB, Sverige

21 Steps to improve Cyber Security of SCADA networks, Department of Energy, USA

ICS Advisory (ICSA-20-289-01) Advantech WebAccess/SCADA, publisert 15.10.2020

Reducing cyber risks for industrial control systems (ICS), Professional Supplementary Document, Cyber Israel

Krysskobling til andre paragrafer og regelverk

§ 5-1. Sikringsplikt

§ 5-2. Klasser

De delene av driftskontrollsystemet som tilhører det sentrale systemet, slik som driftssentraler med tilhørende datarom og hele **sambandsanlegget, som står for seg selv,** er klassifisert etter bestemmelse om driftskontrollssystem i § 5-2.
De delene av driftskontrollsystemet som tilhører en enkelt stasjon, kalt lokalkontroll, er klassifisert etter stasjonens klasse. Grensen mellom lokalkontroll og sentralt system med samband må dokumenteres slik at de forskjellige delene kan sikres etter riktig klasse.
Alle klassifiserte anlegg og system skal sikres, og §§ 5-3. 5-4. 5-5, 5-6 setter krav til fysisk sikring og brannsikring for driftskontrollssystem i forskjellige klasser.
Virksomheter som har et driftskontrollsystem, vil også ha digitale informasjonssystemer. Kravene til grunnsikring av digitale informasjonssystemer ligger i § 6-9. Dette gjelder også for driftskontrollsystemer.
Kravene til sikring av brytefunksjonaliteten i AMS ligger i § 6-10, og det er også krav til sikring av måleverdikjeden i AMS i forskrift om måle- og avregningsforskriftens (MAF) § 4-2.

7.2 Interne sikkerhetsregler

§

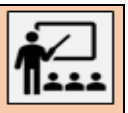
§ 7-2. ***Interne sikkerhetsregler***
Virksomheter skal fastsette sikkerhetsregler for bruk, utvikling, drift, systemvedlikehold, sikring med mer av driftskontrollsystem slik at overvåking og kontroll av kraftforsyningen kan utføres på en sikker måte.

Virksomheter skal gjennomgå sikkerhetsreglene minimum årlig for å sikre at de etterleves og at de gir tilfredsstillende beskyttelse.

Hvordan oppfylle kravet

Virksomheter må omsette forskriftskravene til sikkerhetsregler som er tilpasset virksomheten. Sikkerhetsreglene må sørge for at virksomheten kan overvåke og kontrollere komponenter og anlegg i kraftforsyningen uten at dette arbeidet går på bekostning av sikkerheten. Virksomheten må også definere hva som er sikker drift av driftskontrollsystemet.

Sikkerhetsreglene er virksomhetens eget verktøy for å følge både kravene i forskriften og egne rutiner. Sikkerhetsreglene må være lett tilgjengelig der de skal brukes og bli gjort kjent for brukerne av reglene. Minst en gang i året skal virksomheten gjennomgå sikkerhetsreglene og vurdere behovet for å gjennomføre nødvendige endringer. I dette arbeidet kan det være hensiktsmessig å ta lærdom fra siste års arbeid og rette opp mangler man har erfart, se eksempel på sikkerhetsregler.



Eksempel: Sikkerhetsregler
Kraftkonsernet AS har utarbeidet et sett med sikkerhetsregler for følgende temaer i driftskontrollsystemet:

- ansvarsforhold og sikkerhetsinstruks for driftssentralen
- inndeling i sikkerhetssoner og segmentering av datanettverk
- tilgangsstyring – rollebasert tilgang logisk og fysisk samt passord regler
- hvitelisting av applikasjoner og tilganger – minimering av rettigheter
- styring og kontroll av lisenser
- minimering av eksponering av driftskontrollsystemet på internett
- tilgangsstyring og krav til rettmessige brukere, inklusive brukere hos leverandører
- testing, overvåkning og kontroll av sikkerhet
- sikkerhetskopiering og forsvarlig sletting av driftskritisk informasjon og kraftsensitiv informasjon
- håndtering av og sikring av bevis/dokumentasjon i uønskede hendelser, sikkerhetsbrudd og ekstraordinære situasjoner

Disse temaene er dokumentert, og dokumentene blir gjennomgått årlig for å vurdere relevans og gjennomføre forbedringer.

Standarder
§ 7-2 inneholder deler av mange standarder som et tiltak eller en kontroll:

- NS-EN ISO/IEC 27002:2017 Informasjonsteknologi - Sikringsteknikker - Tiltak for informasjonssikring, se www.standard.no
- ISO/IEC 27002:2017 - Tiltak for informasjonssikring
  - 5.1.1 Policies for information security
  - 5.1.2 Review of the policies for information security
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
  - 4.3.2.6 Security policies and procedures
- NIST 800-100 - Information Security Handbook: A Guide for Managers
  - 2.2.5 Information Security Policy and Guidance
- NERC CIP-003-7 Security Management Controls
  - R1 Cyber security policies

Veiledere
Guide to Increased Security in Industrial Control Systems, MSB, Sverige

21 Steps to improve Cyber Security of SCADA networks, Departement of Energy, USA

Reducing cyber risks for industrial control systems (ICS), Professional Supplementary Document, Cyber Israel

Krysskobling til andre paragrafer og regelverk
§ 2-10 Internkontroll – for klasse 2 og klasse 3 driftskontrollsystem §7-14b.
Sikkerhetsrevisjon
§ 5-1. Sikringsplikt
§ 5-2. Klasser
§§ 5-3. 5-4. 5-5 og 5-6 Sikringstiltak for klassifiserte anlegg avhengig av klasse
§ 6-9 Digitale informasjonssystemer
§ 6-10 Brytefunksjonalitet i avanserte måle- og styringssystem (AMS)
Måle- og avregningsforskriften (MAF) § 4-2 Funksjonskrav

7.3 Dokumentasjon av driftskontrollsystemet

§

§ 7-3. Dokumentasjon av driftskontrollsystemet
Virksomheter skal til enhver tid ha oppdatert dokumentasjon av driftskontrollsystemet.

I dokumentasjonen skal det inngå en oversikt over alle sikkerhetstiltak som er implementert. Dokumentasjonen skal også omfatte en oppdatert skjematisk fremstilling av driftskontrollsystemets logiske og fysiske nettverk som viser eventuelle tilgangspunkt mellom driftskontrollsystemet og andre nettverk. Dokumentasjonen skal også omfatte en komplett oversikt over utstyr i driftskontrollsystemet.

Ordforklaring

Ord	Forklaring
Dokumentasjon	Tegning, bilde eller tekst lagret og gjenfinnbart på digitale medier eller på papir
Logisk nettverk	Logiske nettverk består av: Datanettverk, inkludert IP-adresser, VLAN, subnett, DMZ.
Fysisk nettverk	Geografiske føringer av datakabler, radiolinker, plasseringer av brannmurer, rutere, svitsjer, PLS-er, RTU-er, servere.
Utstyr	Tekniske komponenter og instrumenter, herunder for eksempel dataskjermer, servere, tastatur, PLC, vern, svitsjer, rutere, sensorer mm.
Implementert	Installert og tatt i bruk

Hvordan oppfylle kravet

Dokumentasjonen skal være oppdatert, tilstrekkelig detaljert og relevant slik at brukere av dokumentasjonen ikke er i tvil om egenskaper, konfigurasjon eller innstillinger til datanettverket som benyttes i prosesstyring eller driftskontroll. Dokumentasjonen må sette aktuelle brukere av dokumentasjonen i stand til å gjenopprette driftskontrollsystemet etter feil, svikt eller innbrudd i

systemet. Dokumentasjonen skal være tilgjengelig også uten nettforbindelse, se § 6-8. Dette gjelder både internt og ved fjernlagring.

Den skjematiske fremstillingen skal dekke både det logiske og det fysiske datanettverket. Det skal tydelig komme fram der driftskontrollsystemet er koblet til andre datanettverk som for eksempel administrasjonsnett, leverandør, AMS og Elcom/ICCP.

Formen på dokumentasjonen bør være på et format som fungerer godt for formålet – å kunne drifte og gjenopprette i normal og i ekstraordinære situasjoner. For noen er dette regneark, for andre er det egne systemer, GIS eller tegninger.

Eksempel: Hvordan strukturere dokumentasjon for driftskontrollsystem

Kraftkonsernet AS har følgende dokumentasjon:

- Oversikt over fysiske komponenter (eksempelvis rutere, servere, målere mm.)
    - Produktdokumentasjon fra leverandører av de ulike komponentene i driftskontrollsystemet
- Konfigurasjonsfiler til komponenter, eks. brannmur, IDS, vern
    - Programvare med versjonsnummer
    - Standardinnstillinger og beskrivelse av virksomhetens egne konfigurasjoner av de ulike komponentene
- Systemarkitektur, se Open Systems Interconnection model (OSI model) for lagdeling av digitale systemer
    - Logisk datanettverk med soneinndeling og sikringstiltak, eks. brannmur, innbruddsdeteksjonssystemer (IDS) mv.
    - Fysisk datanettverk
- Beskrivelse av hvordan man fysisk har sikret de ulike komponentene i driftskontrollsystemet

Kraftkonsernet AS har en skriftlig prosedyre for å dokumentere endringer i systemet og en revisjonslogg for dokumentet.

Standarder
§ 7-3 inneholder deler av mange standarder og veiledere som et tiltak eller en kontroll:

- ISO/IEC 27019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyning
  - 8.1.1 Inventory of assets
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
  - 4.2.3.4 Identify the IACS
  - 4.2.3.5 Develop simple network diagrams
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
  - 4.5.1 Categorize ICS Systems and Networks Assets
- NERC CIP-002-5.1a BES Cyber System Categorization
  - R1 Identification and documentation of assets

Veiledere
NSMs Grunnprinsipper for IKT-sikkerhet – Identifisere og dokumentere

Krysskobling til andre paragrafer og regelverk
§ 2-10 setter krav til at det skal dokumenters hvordan forskriftens krav følges, og dokumenteringen av driftskontrollsystemet er en del av dette.
Informasjon om driftskontrollsystemet er kraftsensitiv informasjon etter § 6-2 a og må beskyttes etter kravene i § 6-3.
Det er detaljerte krav til sikkerhetskopier av nødvendig informasjon om driftskontrollsystemet i § 6-8.
§ 6-9 a. har det generelle kravet om å dokumentere verdier og systemer i alle digitale informasjonssystemer.

Eksempel: Registrering av komponenter

For å kunne ha en sikker drift og tilstrekkelig oversikt over driftskontrollssystemet, må dokumentasjonen oppdateres hver gang det kommer nye komponenter inn i systemet eller det gjennomføres en oppgradering av programvare. Dersom Pål Voltersenikke vet hvilken versjon av programvaren som ligger på komponentene kan han heller ikke vurdere sårbarhetsvarsler han får fra KraftCERT (se § 3-6) og bidra til å lukke sårbarheten. Dersom han ikke har oversikt over de tekniske egenskapene til de enkelte enhetene vet han heller ikke om det er skjulte veier inn i systemet, for eksempel en mobilsender/mottaker som ikke er skrudd av eller et standardpassord som ikke er endret.
Pål Voltersen vurderer samtidig kravene til sikkerhetskopier av denne dokumentasjonen.

Digitale systemer trenger å bli oppdatert og feilrettet. Ta kontakt med KraftCERT dersom det er leverandører som ikke varsler om sårbarheter. Da kan KraftCERT følge opp leverandøren. Se § 3-6 og § 6-9.

7.4 Kontroll med brukertilgang

§ 7-4. ***Kontroll med brukertilgang***
Virksomheter skal kontrollere at kun rettmessige brukere har tilgang til driftskontrollsystemet. For dette skal det være kontrollordninger for tildeling, endring og sletting av brukertilgang.

Virksomheter skal kontrollere hvilken bruker som er eller har vært pålogget driftskontrollsystemet, også når ekstern tilkobling brukes.

Kontrollordningene skal gjennomgås minimum årlig for å sikre at alle tilgangsrettigheter er korrekte og på riktig nivå.

Ordforklaring

Ord	Forklaring
Rettmessig bruker	Person eller applikasjon som er godkjent av virksomheten for tilgang
Tilgangsrettighet	En brukers rett til å skrive, endre og lese data
Tilgang	Logisk og fysisk tilgang
Kontrollordning	Fremgangsmåte eller tiltak for å sørge for kontroll

Hvordan oppfylle kravet

Virksomheten må ha en prosedyre for å godkjenne og slette brukere (klarere brukere og autorisere tilgang og rettigheter). Virksomheten må til enhver tid ha oversikt over hvem som har tilgang til driftskontrollsystemet og hvilke handlinger de har lov til å utføre. Virksomheten må også ha en oversikt over - og kunne registrere og kontrollere - hvilke brukere som har vært pålogget eller aktive i driftskontrollsystemet til et hvilket som helst tidspunkt.

Virksomheten må sørge for at brukere ikke har flere rettigheter i domenet til driftskontrollsystemet enn nødvendig. Et minimum av brukere skal ha administratorrettigheter. Å benytte en sentralt styrt brukeradministreringsløsning med rettighetshåndtering, for eksempel Active Directory, vil lette kontrollen med brukerrettigheter i domenet til driftskontrollsystemet.

Eksterne leverandører får ikke lov til å på egenhånd, og uten kontroll fra virksomheten, administrere beskyttelsestiltakene for driftskontrollsystemet. De skal for eksempel ikke oppdatere regelsett for

brannmurer eller konfigurere nettverkssvitsjer uten virksomhetens godkjenning og overvåkning. Sesjoner og endringer skal logges og kunne revideres.

Minst en gang i året skal de forskjellige prosedyrene og kontrollordningene for tilgangsrettigheter gjennomgås. Målsettingen er å sikre at tilgangsrettighetene fortsatt er riktige og prosedyrene relevante. I gjennomgangen skal man også kontrollere at eventuelle endringer og/eller slettinger av tilgang har blitt gjennomført. Merk at tilgangskontroll også inkluderer sikker oppkobling mot driftskontrollsystemet og passordpolitikk. Virksomheten skal også ha kontroll med fysisk tilgang til driftskontrollsystemet, jf. den brede definisjonen av driftskontrollsystemet i § 7-1, og kunne revidere hvem som har hatt tilgang.

NSMs anbefaling for virksomheter:

- Innfør to-faktor autentisering
- Unngå at passord lagres i klartekst
- Innfør rutiner for å kontrollere nye passord mot mye brukte og kompromitterte passord
- Innfør rutiner for å bytte standardpassord på nytt utstyr
- Gi brukere som trenger administratorrettigheter to kontoer

Det finnes også tjenester som https://haveibeenpwned.com/ der domeneeiere og IT-administratorer kan få varsler dersom en epost-adresse i domenet dukker opp i en lekkasje.

Eksempel: Tilgang til driftskontrollsystemet

Nett AS blir revidert av NVE. Revisorene stiller spørsmål om tilgangskontrollen til driftskontrollsystemet. Volt Strøm forklarer at ansatte på driftssentralen har gruppetilgang med felles påloggingsinformasjon. NVEs revisor påpeker at dette ikke er godt nok, det skal være personlige brukere. Om dette ikke er mulig, skal brukeres tilgang og tilstedeværelse registreres i et annet system eller manuelt. Hvem som har hatt tilgang skal være mulig å spore. NVE anbefaler separat Active Directory for driftskontrollsystemet når det er mulig og å følge NSMs passordråd.

Maler

Standarder
§ 7-4 inneholder deler av mange standarder som et tiltak eller en kontroll:

- ISO/IEC 27019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyning
  - 9.1.1 Access control policy
  - 9.1.2 Access to networks and network services
  - 9.2.1 User registration and de-registration
  - 9.2.2 User access provisioning
  - 9.2.3 Management of privileged access rights
  - 9.2.4 Management of secret authentication information of users
  - 9.2.5 Review of user access rights
  - 9.2.6 Removal or adjustment of access rights
  - 9.3.1 Use of secret authentication information
  - 9.4.1 Information access restriction
  - 9.4.2 Secure log-on procedures
  - 9.4.3 Password management systems
  - 9.4.4 Use of privileged utility programs
  - 9.4.5 Access control to program source code
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
  - 4.3.2.6 Security policies and procedures
  - 4.3.3.5 Access control – Account administration
  - 4.3.3.6 Access control – Authentication
  - 4.3.3.7 Access control – Authorization
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
  - 6.2.1 Access control
- NERC CIP-004-6 Personnel and training
  - R4 Access Control
- NERC CIP-007-6 System Security Management
  - R5 System Access Control

Veiledere
NSM Grunnprinsipper for IKT-sikkerhet

- 1.3 Kartlegg brukere og behov for tilgang
- 2.6 Ha kontroll på identiteter og tilganger

NSM Råd og anbefalinger om passord

Krysskobling til andre paragrafer og regelverk
§ 5-11 Restriksjoner for adgang til steder og områder
§ 7-10 Ekstern tilkobling til driftskontrollsystemet
§ 7-14 f Ekstern tilkopling til driftskontrollsystemet for klasse 2 og 3 og § 7-15 c Overvåking og logging for klasse 3 driftskontrollsystem
§7-14c. Overvåkning og logging for klasse 2 og klasse 3 driftskontrollsystem.
§ 6-9 Digitale informasjonssystemer

7.5 Kontroll ved endringer i driftskontrollsystemet

§ 7-5. Kontroll ved endringer i driftskontrollsystemet
Virksomheter skal hindre at utilsiktede feil og nye sårbarheter blir introdusert ved endring i driftskontrollsystemet. For dette skal det være kontrollordninger for vurdering, testing og godkjenning av endringer.

Hvordan oppfylle kravet
Virksomheten må ha forebyggende sikringstiltak og prosedyrer i internkontrollsystemet (ref § 2-10) som beskriver hvordan virksomheten vurderer, tester og godkjenner endringer i driftskontrollsystemet enten det er fysiske endringer eller endringer i programvare. Endring kan inkludere oppdateringer av programvare, konfigurasjonsendringer, oppgradering og utskifting av system eller komponenter. Prosedyrene og tiltakene må legges til grunn for avtalen med leverandører som driver vedlikehold på driftskontrollssystemet.

For å hindre utilsiktede feil og nye sårbarheter, må det utføres tester av at endringen er trygg og at systemet fungerer etter hensikten også etter at endringen er utført.

Før større endringer, for eksempel oppgradering til ny versjon, må virksomheten kartlegge mulige negative konsekvenser som endringen kan medføre. Ved store endringer må det også foreligge en plan for å håndtere uforutsette hendelser som skjer under endringsprosessen.

Virksomheten bør fastsette egne kriterier for hvilke endringer som krever en egen risikovurdering før endringene gjennomføres.

Eksempel: Endringer i driftskontrollsystemet etter varsel fra KraftCERT
Pål Voltersen har mottatt sårbarhetsvarsel fra KraftCERT på en komponent virksomheten har i sitt driftskontrollsystem. KraftCERT skriver i sitt varsel at dette er en kritisk sårbarhet der en mulig angriper kan skaffe seg administrator-brukerrettigheter. KraftCERT anbefaler selskapene å oppdatere programvaren og ta kontakt med leverandøren for mer informasjon.
Pål Voltersen forstår at det er viktig å redusere en så alvorlig sårbarhet i driftskontrollsystemet. SCADA-systemet er duplisert, og oppdateringen utføres av leverandøren og testes først på det ene systemet, før det andre systemet oppdateres.

Maler
Melding om klassifisering av driftskontrollsystem

Standarder
§ 7-5 inneholder deler av mange standarder og veiledere som et tiltak eller en kontroll:

- ISO/IEC 27019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyningen
  - 12.1.2 Change management
  - 12.1.4 Separation of development, testing and operational environments
  - 14.2.1 Secure development policy
  - 14.2.2 System change control procedures
  - 14.2.3 Technical review of applications after operating platform changes
  - 14.2.4 Restrictions on changes to software packages
  - 14.2.8 System security testing
  - 14.2.9 System acceptance testing
  - 14.2.10 ENR – Least functionality
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
  - 4.3.2.6 Security policies and procedures
  - 4.3.4.3 System development and maintanance
- IEC 62443-2-3 – Patch management for the IACS environment
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
  - 6.2.5 Configuration Management
- NERC CIP-007-6 System Security Management
  - R2 Security patch management
- NERC CIP-010-2 Configuration Change Management and Vulnerability Assessments
  - R1 Configuration Change Management

Veiledere

- NSM Grunnprinsipper for IKT-sikkerhet
  - 2.10 Integrer sikkerhet i prosess for endringshåndtering

Krysskobling til andre paragrafer og regelverk
§ 6-9 b. Risikovurdering
§ 7-10 Ekstern tilkopling til driftskontrollsystemet
§ 7-14 f. Ekstern tilkobling til driftskontrollsystemet for klasse 2 og klasse 3 driftskontrollsystem, 7-15c Ekstern tilkobling til driftskontrollsystemet for klasse 3 driftskontrollsystem

7.6 Kontroll med utstyr i driftskontrollsystemet

§

§ 7-6. Kontroll med utstyr i driftskontrollsystemet
Virksomheter skal sørge for at utstyr som benyttes i driftskontrollsystemet ikke har blitt brukt eller blir brukt utenom driftskontrollsystemet, heller ikke midlertidig.

Virksomheter skal hindre urettmessig tilgang mellom driftskontrollsystemet og andre informasjonssystemer.

Virksomheter skal hindre urettmessig tilgang til utstyr som benyttes for å etablere logiske eller fysiske skiller mellom driftskontrollsystemet og andre informasjonssystemer.

Virksomheter skal permanent slette all informasjon i utstyr som ikke lenger skal brukes i driftskontrollsystemet.

Det er ikke tillatt å bruke personlig eid utstyr i driftskontrollsystemet.

Datakommunikasjon i driftssentral og datarom skal være trådbundet.

Beredskapsmyndigheten kan i særskilte tilfeller forby bruk av enkelte typer utstyr.

Ordforklaring

Ord	Forklaring
Logiske skiller	Programvare som inspiserer og stopper ikke godkjent datatrafikk i henhold til forhåndsdefinerte kriterier
Fysiske skiller	Maskinvare, elektroniske komponenter og dørlås, sperringer som begrenser tilgang i henhold til virksomhetens sikkerhetsregler
Trådbundet	Kablet

Hvordan oppfylle kravet

Utstyr som benyttes i driftskontrollsystemet, skal kun benyttes der. Utstyret skal aldri brukes midlertidig i andre nettverk eller til andre oppgaver eller formål. En PC knyttet til administrasjonsnettet eller som er brukt til et annet formål, kan ikke senere benyttes i driftskontrollsystemet. En PC brukt i driftskontrollsystemet kan ikke brukes til noe annet etterpå. Den kan gjenbrukes dersom data er permanent slettet eller lagringsmediene er destruert.

Virksomheten skal sikre at det kun er rettmessige applikasjoner, IP-adresser, maskinvare og personer som har tilgang til driftskontrollsystemet. Utgangspunktet er ingen tilgang, og tilgang gis kun etter godkjenning fra virksomheten (hvitlisting).

Virksomheten skal sørge for at det kun er godkjente brukere som har tilgang til for eksempel brannmur, innbruddsdeteksjon, klienter, svitsjer, låsesystemer etc. Godkjente brukere kan være egne ansatte eller leverandører som drifter systemet eller tjenesten på vegne av, og under kontroll av, virksomheten. Det er virksomheten som bestemmer hvilken tilgang og hvilke rettigheter brukerne skal ha.

Når utstyr eller komponenter ikke lenger skal benyttes i driftskontrollsystemet og heller ikke mellomlagres på sikkert sted som sikkerhetskopi eller reserve, skal informasjonen slettes permanent slik at den ikke kan gjenskapes. Utstyret skal heller ikke gjenbrukes og må derfor destrueres.

Bestemmelsen presiserer at privat utstyr ikke er tillatt å bruke i driftskontrollsystemet. Personlig eid utstyr er ikke omfattet av virksomhetenes sikkerhets- og kontrollregime og kan derfor være mer mottakelig for skadelig programvare og feil.

Med trådløse nettverk menes for eksempel bruk av trådløse rutere (wifi) eller blåtann (Bluetooth) for å overføre nettverkstrafikk basert på bruk av lokale radiosignaler. Trådløs overføring av data er ikke tillatt fordi trådløs kommunikasjon er sårbar for blokkering (interferens mv). På driftssentralen og i datarommet (serverrommet) skal derfor kabler kople sammen servere og klienter, datamus og tastatur.

Bestemmelsen regulerer ikke bruk av radiolinje eller satellittkommunikasjon som samband for overføring av styringssignaler i driftskontrollsystemet.

Eksempel: Kontroll med utstyr som koples til driftskontrollsystemet
Pål Voltersen mener det viktigste tiltaket for å sørge for at utstyr kun blir brukt i driftskontrollsystemet, er å etablere en rutine som beskriver hvordan kravet skal etterleves.
Det er ikke tillatt å benytte privat nettbrett, PC, telefon, mus, lader og minnepinner i driftskontrollsystemet. Dette kravet skrives inn i interne sikkerhetsregler rettet mot ansatte, leverandører og innleide, og dokumenteres i internkontrollsystemet.
Voltersen tar videre utgangspunkt i oversikten han har over alt utstyr i driftskontrollsystemet. Alt utstyr som brukes i driftskontrollsystemet er merket slik at det er enkelt å kjenne igjen for dem som skal bruke det. Utstyret skal videre konfigureres slik at det kun er godkjente komponenter som får bli koplet til driftskontrollsystemet. Rutine for oppdatering av utstyrsoversikter finnes i internkontrollsystemet.

Maler

Standarder

§ 7-6 inneholder deler av mange standarder og veiledere som et tiltak eller en kontroll:

- ISO/IEC 270019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyningen
  - 8.1.1 Inventory of assets
  - 8.1.2 Ownership of assets
  - 8.1.3 Acceptable use of assets
  - 8.1.4 Return of assets
  - 8.2.3 Handling of assets
  - 8.3.1 Management of removable media
  - 8.3.2 Disposal of media
  - 8.3.3 Physical media transfer
  - 11.2.1 Equipment siting and protection
  - 11.2.3 Cabling security
  - 11.2.5 Removal of assets
  - 11.2.6 Security of equipment and assets off-premises
  - 11.2.7 Secure disposal or re-use of equipment
  - 11.2.8 Unattended user equipment
  - 11.3.1 ENR – Equipment sited on the premises of other energy utility organizations
  - 11.3.2 ENR – Equipment sited on customer's premises
  - 11.3.3 ENR – Interconnected control and communication systems
  - 12.8.1 ENR – Treatment of legacy systems
  - 13.1.3 Segregation of networks
  - 13.2.1 Information transfer policies and procedures
  - 14.2.10 ENR – Least functionality
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
  - 4.3.2.6 Security policies and procedures
  - 4.3.3.4 Network segmentation
  - 4.3.4.3 System development and maintanance
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
  - 4.5.1 Categorize ICS Systems and Networks Assets
- NERC CIP-002-5.1a BES Cyber System Categorization
  - R1 Identification and documentation of assets

Veiledere

- NSM sine grunnprinsipper for IKT-sikkerhet
  - 1.2 Kartlegg enheter og programvare
- Nettvett – Metoder for sikker sletting av informasjon, https://nettvett.no/sikker-sletting/

Krysskobling til andre paragrafer og regelverk

§ 7-3 Dokumentasjon av driftskontrollsystemet

§ 2-10 Internkontrollsystem

7.7 Håndtering av feil, sårbarheter og sikkerhetsbrudd

§

§ 7-7.*Håndtering av feil, sårbarheter og sikkerhetsbrudd*
Virksomheter skal håndtere feil, sårbarheter i programvare, sikkerhetsbrudd og andre hendelser som kan utgjøre en risiko for driftskontrollsystemet.

Virksomheter skal ha tilgang til tilstrekkelig personell med nødvendig kompetanse som uten unødig opphold kan håndtere forhold angitt i første ledd.

Virksomheter skal registrere alle sikkerhetsbrudd og -hendelser.

Forhold som kan utgjøre en umiddelbar risiko for driftskontrollsystemets funksjon, skal varsles og rapporteres til beredskapsmyndigheten, jf. § 2-5 og § 2-6.

Hvordan oppfylle kravet

Virksomheten må kunne rette feil, oppdatere programvare, håndtere sikkerhetsbrudd og andre uønskede hendelser slik at virksomheten evner å opprettholde funksjonaliteten til driftskontrollsystemet. For å ha oversikt over sårbarheter, anbefaler NVE virksomhetene å følge med på sårbarhetsvarsler og sikkerhetsråd utsendt fra KraftCERT og fra virksomhetens leverandører.

!

KraftCERT samler informasjon om aktuelle sårbarheter og trusler fra en rekke kilder og videreformidler informasjon og kritiske sårbarheter til virksomheter i kraftbransjen. Virksomheten bør sørge for at IKT-sikkerhetskoordinator eller en annen ansatt abonnerer og følger med på råd fra KraftCERT.

Virksomheten må ha system, programvare og utstyr på plass som bistår med teknisk overvåkning av datanettverk og komponenter, oppdagelse av og varsling av feil og uønskede hendelser. Virksomheten må også ha prosedyre for hendelseshåndtering og feilretting der ansvar og aksjonspunkter framgår. Interne prosedyrer må samkjøres med ekstern leverandørs prosedyrer i supportsituasjoner der det er aktuelt. Merk at avtale om support i helligdager og utenom arbeidstid må inngå i avtalen med leverandøren.

NVE anbefaler at virksomhetene har tilgang til et sikkerhetsoperasjonssenter (SoC), enten eget eller som kjøpt tjeneste. SoC kan overvåke varsler og feilsituasjoner, samt bidra med hendelseshåndtering. KraftCERT kan gi råd i forbindelse med anskaffelse av tjeneste. NSM har en godkjenningsordning for leverandører av sikkerhetstjenester.

Virksomheten må ha tilgang til eget personell med relevant kompetanse eller ha tilgang til kompetent personell gjennom avtale med leverandør. Det kreves ulik kompetanse for å kunne håndtere feil i nett og anlegg kontra det å håndtere IKT-sikkerhetsbrudd. NVE anbefaler virksomhetene å bygge egen tverrfaglig kompetanse på elkraft, operasjonsteknologi (OT) og IKT-sikkerhet. Virksomheten må

uansett ha tilstrekkelig kompetanse til å kunne utforme kravspesifikasjon og følge opp leverandør hvis oppgaven settes ut.

Informasjon om egne sikkerhetsbrudd, herunder logger, må registreres og lagres trygt, beskyttet og med minimal risiko for uautorisert endring, jf. kapittel 6. I noen tilfeller vil sikkerhetsbrudd- og hendelser bli automatisk registrert i flere forskjellige systemer. Hvis ikke informasjon samles i et felles system, må virksomheten ha et dokument som beskriver hvor logginformasjon finnes. Dersom virksomheten opplever sikkerhetsbrudd eller blir utsatt for en kriminell handling, kan tidsseriedata være viktige for etterforskningen. Logger bør lagres minimum to år av hensyn til etterforskningen.

Virksomheten skal varsle NVE dersom det skjer hendelser i driftskontrollsystemet som kan utgjøre en fare for dets funksjon. Det skal foreligge en rutine for slik varsling. Det kan for eksempel være systemfeil som fører til tap av overvåking og kontroll, ikke godkjent tilgang til eller endring av systemet som følge av datainnbrudd. Varsel skal sendes uten ugrunnet opphold jf. § 2-5. Rapport skal sendes etter at hendelsen er håndtert, jf. § 2-6.

I tillegg følger det av § 6-9 c at virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer. NVE har i forventningsbrevet til KBO (20.02. 2020 med referanse tsni) bedt KBO-enhetene varsle KraftCERT om alle uønskede IKT-hendelser. Dette er en praktisk ordning for KBO og NVE. Deling av opplysninger om hendelser og suspekt aktivitet med KraftCERT vil være til nytte for etablering av et mer detaljert situasjonsbilde. Gjennom høy delaktighet og lav terskel for å dele, vil den kollektive evnen til læring og beskyttelse blir bedre. § 2-5 og § 2-6 gir bestemmelser om hendelser som skal varsles og rapporteres til NVE. Merk at kraftsensitiv informasjon må beskyttes som angitt i kapittel 6.

Standarder

- ISO/IEC 27019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyningen
  - 16.1.1 Incident management – Responsibilities and procedures
  - 16.1.2 Reporting information security events
  - 16.1.3 Reporting information security weaknesses
  - 16.1.4 Assessment of and decisions on information security events
  - 16.1.5 Response to information security incidents
  - 16.1.6 Learning from information security incidents
  - 16.1.7 Collection of evidence
  - 12.2.1 Controls against malware
  - 12.4.1 Event logging
  - 12.6.1 Management of technical vulnerabilities
  - 17.1.1 Planning information security continuity
  - 17.1.2 Implementing information security continuity
  - 17.1.3 Verify, review and evaluate information security continuity
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
  - 4.3.2.6 Security policies and procedures
  - 4.3.4.3 System development and maintainence
  - 4.3.4.5 Incident planning and response
- IEC 62443-2-3 – Patch management fir the IACS environment
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security

- 6.2.6 Contingency planning
- 6.2.8 Incident response

- NERC CIP-008-5 Incident reporting and response planning
  - R1, R2, R3 Cyber security incident response plan
- NERC CIP-009-6 Recovery Plans for BES Cyber systems
  - R1, R2, R3 Recovery plan

Veiledere

- NSM sine grunnprinsipper for IKT-sikkerhet
  - 3.2 Etabler sikkerhetsovervåkning
  - 4 Håndtere og gjenopprette

- Logging og logganalyse i energiforsyningen. Studentrapport. NVE-rapport 1:2017
- Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem. Rapport utarbeidet av BDO AS for Norges vassdragsog energidirektorat, NVE-rapport 14:2017

Krysskobling til andre paragrafer og regelverk
§ 2-4 Beredskapsplanlegging
§ 2-5 Varsling
§ 2-6 Rapportering
§ 4-1 Reparasjonsberedskap
§ 4-2 Kompetanse og personell
§ 4-4 Materiell og utstyr
§ 6-9 Digitale informasjonssystemer
§ 7-14 c Overvåkning og logging – for klasse 2 og 3 driftskontrollsystem

7.8 Beredskap ved svikt i driftskontrollsystemet

§

§ 7-8. Beredskap ved svikt i driftskontrollsystemet
Virksomheter skal ha beredskap og forberedte tiltak for fortsatt drift av anlegg ved svikt i driftskontrollsystemet.

Hvordan oppfylle kravet

Bestemmelsen stiller krav til at virksomheten skal ha forberedt nødvendige tiltak for å drifte sine anlegg selv om driftskontrollsystemet er degradert eller slutter å virke. Virksomheten må derfor ha en beredskapsplan som beskriver hvordan driften av anleggene skal gjøres i en slik situasjon og ikke minst hvordan virksomheten skal få gjenopprettet systemet igjen. I dette inngår å reetablere ved å benytte sikkerhetskopier og installere systemet på nytt dersom det er behov for det.

Planen bør inneholde en beskrivelse av hvordan anleggene skal driftes dersom driftskontrollsystemet blir utilgjengelig over lengre tid (dager, uker). Den bør beskrive ansvar, kontaktinformasjon og plan for bemanning av anleggene over tid slik at anleggene kan styres manuelt ved behov. Se også vedlegg 2 og 3 i beredskapsforskriften (pkt. 2.1.4 og 3.1.4). Beredskapsplanen bør også inkludere prosedyrer

for driftskommunikasjon og kommunikasjon med virksomhetens ledelse dersom lokal bemanning og manuell styring er nødvendig. Beredskapsplanen bør også henvise til hvor man finner nødvendig systeminformasjon, eventuelt papirkopier av kritisk informasjon.

Manuell styring krever kompetanse som ikke blir brukt til daglig. Manuell styring av anlegg må derfor være forberedt og inngå som en del av øvelsesplanen til selskapet etter § 2-7 jf. § 7-14 d. NVE anbefaler å øve med et representativt anlegg, og om mulig rullere på anlegg og personell, og ha ulike scenarier.

Maler

Standarder

- IEC 62443-2-1 – Establishing an industrial automation and control system security program
  - 4.3.4.5 Incident planning and response
- IEC 62443-2-3 – Patch management for the IACS environment
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
  - 6.2.6 Contingency planning
  - 6.2.8 Incident response
- NERC CIP-008-5 Incident reporting and response planning
  - R1, R2, R3 Cyber security incident response plan
- NERC CIP-009-6 Recovery Plans for BES Cyber systems
  - R1, R2, R3 Recovery plan

Veiledere

- NSM Grunnprinsipper for IKT-sikkerhet
  - Håndtere og gjenopprette

Krysskobling til andre paragrafer og regelverk
§ 2-4 Beredskapsplanlegging
§ 4-3 Drift i ekstraordinære situasjoner og gjenoppretting av funksjon
§ 7-14 d. Utilgjengelig driftssentral - klasse 2 og 3 driftskontrollsystem

7.9 Bemanning av driftssentral

§ 7-9. Bemanning av driftssentral
Virksomheter skal til enhver tid ha tilstrekkelig og tilgjengelig autorisert personell med nødvendig kompetanse, slik at driftskontrollfunksjonen kan utøves uten ugrunnet opphold.

Virksomhetens risikovurdering skal ligge til grunn for valg av bemanningens størrelse samt omfang av ordninger for påkalling av ekstra personell ved behov, jf. § 2-4 og § 5-8.

Ordforklaring

Ord	Forklaring
Autorisert	Godkjent av virksomheten – funnet kvalifisert og sikkerhetsmessig egnet

Hvordan oppfylle kravet

Virksomheten skal gjøre en vurdering av hva som er nødvendig kompetanse for å utføre jobben og autorisere personell som har kvalifikasjoner og er sikkerhetsmessig egnet. Virksomheten må også ha en prosedyre for å godkjenne personell som skal arbeide som operatør i driftssentralen og gi nyansatte og fast ansatte ved driftssentralen tilstrekkelig opplæring og trening. Læring skjer gjennom daglig arbeid, kurs og øvelser.

Virksomheten skal ha en prosedyre for å vurdere i hvilken grad bemanningen er tilstrekkelig for å betjene driftssentralen, og i hvilken grad påkallingsordningens omfang er tilstrekkelig. Til grunn for vurderingene skal virksomheten gjøre en risikovurdering. Dette er et grunnleggende krav for alle KBO-enheter med driftskontrollsystemer eller virksomheter med driftskontrollsystemer der NVE har fattet vedtak om at virksomheten underlegges kravet. Det er tilleggskrav for driftskontrollsystemer i klasse 2 og 3, se §§ 7.14 d og e, og -7-15 b.

Kompetanse for personell som utøver driftskontrollfunksjoner:

- Fagkunnskap tekniske anlegg og om driftskontrollsystemet
- Oversikt over forsyningsområdet
- Inngående kjennskap til virksomhetens beredskapsplanverk og prosedyrer for håndtering av kompliserte feilsituasjoner
- Kompetanse i krisehåndtering (kan opparbeides gjennom øvelser)
- Språkkunnskaper i norsk og engelsk

Veiledere

- NSR, Politiet, NSM, Sikkerhet ved ansettelsesforhold
- NSM Temarapport Innsiderisiko,

Standarder

Krysskobling til andre paragrafer og regelverk
§ 2-4 Beredskapsplanlegging
§ 2-10 Internkontroll
§ 4-2 Kompetanse og personell
§ 7-14 e Bemanning av driftssentral
§ 7-15 b Bemanning av driftssentral

§ 5-8 Vurdering
§ 6-7 Personkontroll
Det er tilleggskrav for driftskontrollsystemer i klasse 2 og 3, se §§ 7.14 d
Utilgjengelig driftssentral, e Bemanning av driftssentral, og 7-15 b Systemredundans.

7.10 Ekstern tilkobling til driftskontrollssystemet

§

§ 7-10. ***Ekstern tilkobling til driftskontrollsystem***
Virksomheter skal ha kontroll med ekstern tilkobling til driftskontrollsystemet.

Kun godkjente brukere kan gis tilgang til driftskontrollsystemet gjennom ekstern tilkobling. Virksomheter skal ha en oppdatert liste over alle godkjente brukere.

Det skal foreligge en egen forhåndsavtalt prosedyre for ekstern tilkobling til driftskontrollsystemet.

Virksomheter skal ha kontrollordninger for å godkjenne, vedlikeholde og avvikle ordninger for ekstern tilkobling til driftskontrollsystemet, og for funksjoner for innstilling av vern.

Virksomheter skal ha kontrollordninger for vurdering, tildeling, endring og tilbaketrekking av brukertilgang.

Hvordan oppfylle kravet

Tilkobling til et driftskontrollsystem fra en applikasjon, tjeneste eller maskin, fra bruker på hjemmekontor eller fra en bruker hos en leverandør i dennes lokaler, er en ekstern tilkobling. Ekstern tilgang skal normalt være stengt og kun åpnes når det er behov. Med tilgang menes her logisk tilgang.

Virksomheten kan oppfylle kravet om å ha kontroll ved å sørge for at tilgang til driftskontrollsystemet må godkjennes på forhånd av personell som virksomheten har bemyndiget. Virksomheten må ha prosedyrer for å godkjenne brukere, administrere logisk tilgang og brukerrettigheter.

Virksomheten må ha en prosedyre som beskriver forløpet fra operatør på driftssentralen gir tilgang til ekstern tilkopling og til den eksterne tilkoplingen er lukket.

Det skal til enhver tid være en oppdatert liste over brukere (personer, applikasjoner og maskinvare) som virksomheten har gitt tillatelse til å koble seg på driftskontrollsystemet.

Virksomheten må ha prosedyre i kombinasjon med tekniske tiltak og personelltiltak for å godkjenne, vedlikeholde og avvikle tilgang til driftskontrollsystemet. Tekniske tiltak kan være hvitelisting (forhåndsgodkjenning av maskiner, MAC-adresser, IP-adresser, programvare, protokoller m.m.), multifaktor-autentisering av brukere, pålogging og kommunikasjon over sikret kanal, rettighets- og tilgangsstyring og andre tiltak som for eksempel begrensning i antall feilpåloggінger før muligheten stenges, tidsbegrenset tilgang, overvåkning og logganalyse. Personelltiltak omfatter identifisering,

klarering og autorisasjon, bakgrunnssjekk og godkjenning av kvalifikasjoner og egnethet; se også § 6-7.

Virksomheten må ha en prosedyre for å vurdere behov for brukertilgang og tilhørende risiko. Virksomheten må ha prosedyrer for å tildele, endre og slette tilgang og rettigheter i driftskontrollsystemet.

Veiledning

- NSM Grunnprinsipper for IKT-sikkerhet
  - 1.3 Kartlegg brukere og behov for tilgang
  - 2.2 Etabler en sikker IKT-arkitektur
  - 2.4 Beskytt virksomhetens nettverk
  - 2.5 Kontroller dataflyt
  - 2.6 Ha kontroll på identiteter og tilganger

Standarder

- ISO/IEC 27019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyningen
  - 6.2.2 Teleworking
  - 9.1.1 Access control policy
  - 9.1.2 Access to networks and network services
  - 9.2.1 User registration and de-registration
  - 9.2.2 User access provisioning
  - 9.2.3 Management of privileged access rights
  - 9.2.4 Management of secret authentication information of users
  - 9.2.5 Review of user access rights
  - 9.2.6 Removal or adjustment of access rights
  - 9.3.1 Use of secret authentication information
  - 9.4.1 Information access restriction
  - 9.4.2 Secure log-on procedures
  - 9.4.3 Password management systems
  - 9.4.4 Use of privileged utility programs
  - 9.4.5 Access control to program source code
  - 11.3.1 ENR – Equipment sited on the premises of other energy utility organizations
  - 11.3.2 ENR – Equipment sited on customer's premises
  - 11.3.3 ENR – Interconnected control and communication systems
  - 13.1.5 ENR – Logical connection of external process control systems
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
  - 4.3.2.6 Security policies and procedures
  - 4.3.3.3 Physical and environmental security
  - 4.3.3.4 Network segmentation
  - 4.3.3.5 Access control – Account administration
  - 4.3.3.6 Access control – Authentication
  - 4.3.3.7 Access control – Authorization
- IEC 62443-3-3 – System security requirements and security levels
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
  - 6.2.1 Access Control

- 6.2.2 Awareness and training
- 6.2.7 Identification and Authentication
- 6.2.16 System and Communications Protection

- NERC CIP-004-6 Personnel and training
  - R4 Access Control
- NERC CIP-007-6 System Security Management
- R5 System Access Control

7.11 Systemredundans i driftskontrollsystemet

§

§ 7-11. Systemredundans i driftskontrollsystemet
Virksomheter skal vurdere behovet for redundans i driftskontrollsystemet basert på lokale forhold og risikovurdering.

Ordforklaring

Ord	Forklaring
Redundans	Reservekapasitet/dublering av kritiske komponenter og funksjoner for å øke påliteligheten til systemet

Hvordan oppfylle kravet

Kravet betyr at virksomheten må vurdere behovet for redundans i driftskontrollsystemet. Vurderingen skal ta utgangspunkt i en risikovurdering av driftskontrollsystemet. Virksomheten må derfor kartlegge risiko for enkeltfeil og identifisere de tilfeller der enkeltfeil medfører uakseptabel konsekvens. I disse tilfellene skal redundans som forebyggende tiltak vurderes, men det er mulig å velge andre tiltak enn redundans.

Redundans kan oppnås ved å dublere kommunikasjonslinjer i risikoutsatte områder, ved å ha dublert kritiske komponenter eller prosessmaskiner. Redundans reduserer risikoen for alvorlig svikt i driftskontrollssystemet ved en enkelt feil i en enkelt komponent eller en maskin.

Dersom virksomheter med driftskontrollsystem i klasse 1 vurderer at det er behov for redundans, bør de iverksette tiltak som styrker redundansen. Dersom virksomheter med driftskontrollsystem i klasse 1 vurderer at det ikke er behov for redundans, er virksomheten likevel pålagt kompenserende tiltak i form av reparasjonsberedskap (se kapittel 4 og forskriftens vedlegg 1). For virksomheter i klasse 2 og 3 er kravet til redundans tydeligere, se § 7-14 g og h, og § 7-15 d.

Eksempel: Risikoanalysen viser behov for redundante linjer
Risikoanalysen til Kraftkonsernet AS viser at en av linjene går i et rasutsatt område. I dag er det bare en linje til klasse 2 transformatorstasjon som forsyner mange med strøm. Risikoanalysen konkluderer med at risikoen for ras vil øke i tiden framover som følge av klimatiske endringer. Kraftkonsernets ledelse beslutter derfor å bygge en alternativ kommunikasjonslinje til denne transformatorstasjonen som går utenfor rasområdet. De setter i gang et arbeid med å utrede radiolinje eller bruk av offentlig mobilnett som redundant kommunikasjon til transformatorstasjonen.
På en annen strekning med kommunikasjon til en klasse 1 stasjon, er også risikoen høy. Her vurderer virksomheten å heller etablere reparasjonsberedskap.

Maler

Standarder
NIST, Guide to Industrial Control Systems (ICS) Security
ISO/IEC 27019:2017 - Information technology — Security techniques — Information security controls for the energy utility industry

Veiledning
MSB, Guide to Increased Security in Industrial Control Systems

Krysskobling til andre paragrafer og regelverk
Kbf §§ 2-3, 5-8 og 6-9 stiller krav til risikovurdering, som vurdering av redundans er en del av
Kbf § 2-10 Internkontroll.
Det kan være nyttig å se på kravene til redundans og dublering i vedlegg 2 og 3 til §§ 5-5 og 5-6 i forskriften. Vedleggene kommer bak i forskriften.
Klasse 2 og 3 driftskontrollsystemer har tilleggskrav om redundans i § 7-14 g.
Klasse 3 driftskontrollsystemer har tilleggskrav om redundans i § 7-15 a og d.
Kapittel 4s krav til reparasjonsberedskap

7.12 (Opphevet)

Denne paragrafen er opphevet 1.1.2019.

7.13 Beskyttelse mot elektromagnetisk puls og interferens

§

***§ 7-13.*Beskyttelse mot elektromagnetisk puls og interferens**

Virksomheter skal vurdere driftskontrollsystemets sårbarhet for elektromagnetisk puls (EMP) eller elektromagnetisk interferens (EMI). Dersom sårbarheter avdekkes, skal det gjennomføres sikrings- eller beredskapstiltak etter driftskontrollsystemets betydning for sikker drift og gjenoppretting av funksjon i kraftforsyningen.

Ordforklaring

Ord	Forklaring
Elektromagnetisk puls (EMP)	EMP omfatter alle elektriske forstyrrelser med kort varighet. EMP transmitteres både som elektromagnetisk stråling og som ledningsbåren strømpuls. EMP fra lynutladninger omtales som LEMP (L = Lightning) og EMP fra kjerneeksplosjoner betegnes NEMP (N = Nuclear). NEMP er ca. 1000 ganger raskere enn LEMP
Elektromagnetisk interferens (EMI)	Elektromagnetisk interferens, betegnelse på forstyrrelser og støy i elektronisk utstyr som skyldes elektromagnetisk påvirkning fra omgivelsene, enten denne kommer i form av radiobølger eller via ledninger
Tilsiktet (intentional) elektro-magnetisk interferens (IEMI)	Elektromagnetisk forstyrrelse forårsaket av radiofrekvente våpen (RFV) med mikrobølgekilder. 18 GHz utgjør en øvre teoretisk grense for funksjonsforstyrrelser eller ødeleggelse av elektronisk utstyr, mens 10 GHz utgjør en øvre grense for praktisk utforming av radiofrekvente våpen. Virkningen dekker et meget begrenset geografisk område, i praksis kanskje bare opptil 100 m. Energien kan – på tilsvarende måte som for EMP – forplante seg som stråling eller være ledningsbundet. En smalspektret puls kan ha svært høy pulseffekt, selv om det totale energiinnholdet er lavt. Det største skadepotensialet ligger i utnyttelse av resonans. En bredspektret puls har mye lavere spektraleffekt, og er mer egnet til å skape forstyrrelser enn forårsake varig skade

Hvordan oppfylle kravet

Virksomheten skal vurdere driftskontrollsystemets sårbarhet for elektromagnetisk puls og elektromagnetisk interferens. Definisjonen av driftskontrollsystemet er vid, jf. § 7-1: Driftskontrollsystemer omfatter driftssentraler, utstyr, nettverk, datarom, sambandsanlegg og øvrige anlegg og rom, systemer og komponenter som ivaretar driftskontrollfunksjoner.

Virksomheten må gjøre en samlet vurdering av risiko og behov for EMP- og EMI-sikring i driftskontrollsystemet. Basert på risikovurderingen må virksomheten ha en overordnet strategi for hvordan sikring gjennomføres. Et sentralt driftskontrollsystem som styrer mange lokalkontrollanlegg vil kreve høy driftspålitelighet (oppetid), mens andre mindre kritiske funksjoner, eksempelvis lokalkontrollanlegg, kan tillates å falle ut en kort tid, andre igjen kan ha avbrudd noe lengre tid uten at det får konsekvenser for kraftforsyningen, eksempelvis dublert kommunikasjonsvei. Tiltak vil kunne være jording, skjerming, avledning og filtrering, alternativt reservedeler eller prosedyre for manuell styring direkte i kontrollanlegget.

Veiledning
SINTEF Energiforskning. EMP-sikring av kraftforsyningsanlegg: Håndbok. Lysaker: Energiforsyningens fellesorganisasjon, 2000

Forsvarsbygg. *EMP-handbok: Veiledning i sikring av kritisk infrastruktur mot elektromagnetiske effekter*. Oslo: Forsvarsbygg, 2020. (Distribusjon ved henvendelse til NVE eller Forsvarsbygg)

Beskyttelse av elektroniske installasjoner i totalforsvaret mot elektromagnetisk puls (EMP), retningslinjer fastsatt av Samferdselsdepartementet 24.03.1998.

Krysskobling til andre paragrafer
Driftskontrollsystemer i klasse 2 og 3 har tilleggskrav om EMP og EMI i kbf § 7-14 i.
Driftskontrollsystemer i klasse 3 har tilleggskrav om EMP og EMI i kbf § 7-15 e.

7.14 Særskilte krav til driftskontrollsystemer i klasse 2

§ 7-14.Særskilte krav til driftskontrollsystem klasse 2
Foruten de generelle krav til beskyttelse av driftskontrollsystemet, skal virksomheter med driftskontrollsystem i klasse 2 oppfylle følgende tilleggskrav:

a. Sikkerhetskopier
Virksomheten skal jevnlig teste at gjenoppretting av elektroniske sikkerhetskopier fungerer etter hensikten

b. Sikkerhetsrevisjon
Virksomheten skal jevnlig gjennomføre en sikkerhetsrevisjon og kontroll av pålagte beskyttelsestiltak i driftskontrollsystemet. Revisjonens formål skal være å påse at tiltakene faktisk er etablert og fungerer etter sin hensikt

c. Overvåking og logging
Virksomheten skal ha automatisk overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i driftskontrollsystemet

d. Utilgjengelig driftssentral
Dersom driftssentralen blir utilgjengelig, skal virksomheten kunne betjene og manuelt styre anlegg som inngår i virksomhetens driftskontrollsystem. I tillegg skal virksomheten ha planer for alternativ drift dersom driftssentralen blir utilgjengelig over lengre tid

e. Bemanning av driftssentral

Virksomheten skal sørge for at alle påregnelige ekstraordinære situasjoner eller hendelser i energisystemet eller i driftskontrollsystemet umiddelbart oppdages og håndteres uten unødig opphold

Virksomheten skal senest innen én time kunne bemanne driftssentralen.

Virksomheten skal ha en vaktordning som til enhver tid sikrer rask opptrapping av bemanningen ved behov.

f. Ekstern tilkobling til driftskontrollsystemet

Ved tilkobling fra leverandører skal driftssentralen være bemannet

Virksomheter skal ha kontrollordning for korrekt verifisering av de brukere som er godkjent til å benytte ekstern tilkobling for tilgang til driftskontrollsystemet. Det er ikke tillatt at én brukeridentitet deles mellom flere personer eller systemer.

Virksomheter skal sørge for at ekstern tilkobling utføres fra et sted med tilstrekkelig sikre omgivelser. Virksomheter skal utarbeide interne regler for hva som er et sikkert sted.

Den eksterne tilkoblingen skal kun åpnes når det er behov for å få tilgang til driftskontrollsystemet. Tilkoblingen skal være lukket når den ikke er i bruk.

Det skal foreligge en egen skriftlig prosedyre for ekstern tilkobling.

Dersom KBO-enheten kan foreta styring av anlegg i kraftforsyningen gjennom ekstern tilkobling, skal styringen kun skje etter tillatelse eller retningslinjer fra bemyndiget person.

Enhver påkobling til driftskontrollsystemet gjennom ekstern tilkobling skal loggføres.

g. Systemredundans

Samband i driftskontrollsystemet skal fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett

Driftskontrollsystemet frem til anlegg i klasse 2 og 3 skal være redundant frem til det lokale kontrollanlegget. I det lokale kontrollanlegget skal virksomheten vurdere behovet for redundans.

Redundante føringsveier for samband og redundante komponenter i driftskontrollsystemet skal være fysisk adskilte og uavhengige slik at én enkelt feil eller hendelse ikke medfører tap av viktige funksjoner.

Det skal etableres reparasjonsberedskap for alt samband, jf. kapittel 4 og § 7-8.

h. Særskilt om dublering

Ved dublering som benytter identiske teknologier og løsninger i driftskontrollsystemet, må virksomheten innrette seg slik at samme systemfeil ikke rammer alle dublerte system samtidig, jf. § 7-7

i. Beskyttelse mot EMP og EMI

Det skal gjennomføres sikrings- eller beredskapstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 2 og 3 som driftskontrollsystemet styrer

j. Sikker tidsreferanse
Driftskontrollsystem som er avhengig av eksakt tidsreferanse, skal ha sikre kilder for tidsangivelse

k. Krav til leverandører
For leveranser til driftskontrollsystemer tillates kun utenlandske leverandører fra land som er medlem i EFTA, EU eller NATO. En leveranse omfatter levering av utstyr, komponenter, programvare, data, programmeringstjenester, oppdateringer, feilretting, service og vedlikehold

Hvordan oppfylle kravet

Kravene i § 7-14 er detaljerte tilleggskrav til klasse 2 driftskontrollsystemer. Disse kravene kommer i tillegg til grunnkrav som er oppstilt tidligere i kapittel 7 i forskriften.

Bokstav a

§ 7-14a. Sikkerhetskopier gjelder elektroniske sikkerhetskopier som kan brukes til å gjenopprette systemet etter ekstraordinær hendelse, for eksempel utilsiktet systemsvikt eller angrep med krypteringsvirus. Sikkerhetskopiene må lagres trygt og være beskyttet mot all ikke autorisert endring. Prosedyre for testing av sikkerhetskopier bør inngå i internkontrollsystemet og testing bør gjøres minimum årlig. Kravet bygger videre på § 7-8, se også § 4-1 Reparasjonsberedskap§ 7-3 Dokumentasjon av driftskontrollsystemet og § 6-8 Sikkerhetskopi.

Bokstav b

§ 7-14 b. Sikkerhetsrevisjon skal gjennomføres jevnlig for å teste at pålagte tiltak faktisk er etablert og fungerer. NVE anbefaler at sikkerhetsrevisjon gjøres årlig og inngår i virksomhetens årsplan.

Bokstav c

§ 7-14c. Overvåkning og logging bygger på § 7-7. Logger knyttet til brukeraktivitet bør lagres i minst 2 år av hensyn til etterforskning av uønskede hendelser der en angriper kan skjule sin aktivitet i systemet i lengre tid. Hensikten med bestemmelsen er at virksomheten ved tidlig varsling til KraftCERT (jf § 2-5) om uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet kan hindre tap av funksjon i driftskontrollsystemet eller få satt i gang feilsøking og feilretting raskest mulig.

Virksomheten må ha et system som automatisk overvåker trafikk i nettverk og som gir alarm eller varsler ved unormal aktivitet. Bestemmelsen må ses i sammenheng med kravet om å etablere effektive reaksjonsrutiner for å håndtere feil, sårbarheter og sikkerhetsbrudd i driftskontrollsystemet i § 7-7. Håndtering av feil, sårbarheter og sikkerhetsbrudd.

Installering, konfigurering og innstillinger av alarmer og monitoreringsparametre i overvåkingssystem eller i brannmurer eller svitsjer kan være komplisert, og øker i kompleksitet med størrelse og omfang på driftskontrollsystemet. Blir systemene konfigurert feil, risikerer man å få mange falske alarmer, men også at systemene stopper «lovlig» trafikk i driftskontrollsystemet eller ikke beskytter systemet som tiltenkt.

NVE anbefaler at virksomheten samarbeider med leverandøren av driftskontrollsystemet når den skal etablere automatiske overvåkings- eller beskyttelsessystem i driftskontrollsystemet. På den måten kan man unngå at funksjonalitet i driftskontrollsystemet blir forstyrret eller hindret ettersom overvåkingssystemene også kan forstyrre normal datatrafikk.

Hvis systemet krever at man utplasserer sensorer i nettverket, må man passe på at disse ikke forstyrrer signalene for å overvåke og styre anleggene. En måte å gjøre det på, kan være å plassere sensorer utenfor selve driftskontrollsystemet slik at man ikke foretar analyse i datanettverket til driftskontrollsystemet.

Bokstav d

§ 7-14 d stiller krav til at virksomheten med klasse 2 driftssentraler skal kunne drifte systemet selv om driftssentralen blir utilgjengelig. Kravene bygger videre på kravet i § 7-8 Beredskap ved svikt i driftskontrollsystemet og gir flere føringer for løsningen.

Bokstav e

§ 7-14 e Bemanning av driftssentral stiller detaljert krav til bemanning og styrking av driftssentral i klasse 2 driftskontrollsystemer. Kravet kommer i tillegg til § 7-9 Bemanning av driftssentral.

Bokstav f

§ 7-14 f. Ekstern tilkopling til driftskontrollsystemet er tilleggskrav til § 7-10 Ekstern tilkopling. Kravene er detaljerte og gir flere føringer. Virksomheten må selv vurdere hva som er tilstrekkelig sikre omgivelser og sikkert sted. NVE vurderer offentlig rom (flyplasser, kjøpesentre, hoteller) som ikke-sikkert sted, fordi det ikke er begrensninger med hensyn til hvem som kan ha adgang. Dersom en må koble til driftskontrollsystemet utenfor leverandørens eller virksomhetens lokaler, er det viktig at det er iverksatt gode sikringstiltak som beskytter både opp- og nedkobling, samt overføring av data, mot avlytting og manipulasjon.

Bokstav g

§ 7-14g Systemredundans kommer som tilleggskrav til § 7-11. Mens § 7-11 setter krav til å vurdere behovet og velge aktuelle tiltak for å håndtere risikoen, så er kravene i § 7-14g detaljkrav som styrker sikkerheten og begrenser valgfriheten. Kravet er spesielt strengt når det gjelder samband (elektronisk kommunikasjon) og redundans. Samband skal fungere uavhengig av svikt i det offentlige elektroniske kommunikasjonssystemer. NVE godtar at en sambandsvei i en redundant løsning går via offentlige elektroniske kommunikasjonsnett.

Bokstav h

§ 7-14 h Særskilt om dublering bygger også videre på § 7-11 og detaljerer krav til å redusere risikoen for at samme feil rammer redundante systemer. Kravet er at sikringstiltak skal hindre at en feil, eksempelvis skadevare, smitter på reservesystemet. Dersom en ikke benytter ulike teknologier fra for eksempel ulike leverandører, må risikoen håndteres gjennom andre forebyggende tekniske og organisatoriske sikringstiltak. Eksempler er rutiner for uttesting av programvare før oppdatering, sikkerhetskopier, planlagt og testet backup, reserveløsninger og prosedyrer for manuell drift.

Bokstav i

§ 7-14 i Beskyttelse mot EMP og EMI bygger videre på § 7-13 og setter i tillegg krav til EMP- og EMI-sikring av minst en sambandsvei fra driftskontrollsystemet til anlegg i klasse 2 og 3.

All elektronikk, inkludert sambandsutstyr og datautrustning tilhørende driftskontrollsystemer, er i utgangspunktet meget sårbart for ekstreme elektromagnetiske hendelser som HEMP og IEMI. Kraftkomponenter (transformatorer mv), vern og instrumentering er langt mer robuste, men overgangen til digitalt instrumenterte transformatorstasjoner i friluft, gir sårbarhet for vern og instrumentering. EMP- og EMI-beskyttelse vil begrense skadevirkningene dersom trusselen inntreffer.

Behovet for beskyttelse mot HEMP E1 er minimum 30 dB demping for frekvenser opp til 1 GHz. Behovet for beskyttelse mot HEMP E1 og IEMI kombinert er minimum 30 dB demping for frekvenser opp til 10 GHz.

Beskyttelsesnivået vil ikke forhindre funksjonsfeil, forstyrrelser og mulig avbrudd, men forhindre varig skade på elektronisk utstyr og datautrustning.

Anlegg med fjelloverdekning på minst 10 meter er naturlig sikret mot strålingsfelt fra HEMP E1 og IEMI, men behovet for vern mot transiente overspenninger på kabler og ledningsnett må vurderes.

HEMP vil ramme mange anlegg samtidig. Beskyttelsen består i et tilstrekkelig robust kraftsystem som kan motstå skadevirkningene. IEMI er derimot en potensiell trussel kun mot enkeltanlegg eller deler av driftskontrollsystemet. IEMI-trusselen kan antas å være størst for de mest kritiske anleggene, og mest relevant for anlegg med fri sikt og enkel adkomst med kjøretøy. Sårbarheten for IEMI-trusler er avhengig av redundansen i kraftsystemet, antatt skadeomfang og medgått tid for gjenoppretting av systemredundans.

Krav om beskyttelse mot HEMP E1 omfatter i utgangspunktet alle installasjoner i driftskontrollsystemer i klasse 2 og 3, og alle lokalkontrollanlegg for kraftforsyningsanlegg i klasse 2 og 3. Tilleggsbeskyttelse mot IEMI bør omfatte alle installasjoner i driftskontrollsystemer og lokalkontrollanlegg med fri sikt og enkel adkomst.

Tiltakene omfatter skjerming, jording og avledning, eventuelt i kombinasjon med soneinndeling. For planlegging, utførelse og testing henvises til relevante standarder og veiledere nedenfor.

EMP-sikring vil vanligvis måtte omfatte:

- Lokalkontrollanlegg for kraftforsyningsanlegg i klasse 2 og 3
- Minst én sambandsvei til kraftforsyningsanlegg i klasse 2 og 3. For sambandsvei til kraftforsyningsanlegg i klasse 2 kan EMP-beredskap aksepteres
- Datarom, sambandsrom og driftssentral (kontrollrom) for driftskontrollsystemer i klasse 2 og 3, inkludert systemer for sikkerhetskopiering og løsninger/installasjoner for alternativ drift. Utstyr som ikke befinner seg i EMP-sikre rom, må kunne erstattes raskt av utstyr som ikke er påvirket av den samme hendelsen
- Avbruddsfri strømforsyning og nødstrømsaggregat (alternativt EMP-resistent aggregat eller EMP-beredskap for styreelektronikk)
- Adgangskontrollsystemer og systemer for elektronisk overvåkning

Maler

Standarder

IEC 61000 serien om elektromagnetisk kompatibilitet
IEC/TR 61000-1-3:2002: Electromagnetic compatibility (EMC) – Part 1-3: General – The effects of high-altitude EMP (HEMP) on civil equipment and systems.

IEC/TR 61000-1-5:2004: Electromagnetic compatibility (EMC) – Part 1-5: General – High power electromagnetic (HPEM) effects on civil systems.
IEC 61000-2-9:1996: Electromagnetic compatibility (EMC) – Part 2: Environment – Section 9: Description of HEMP environment – Radiated disturbance.
IEC 61000-2-10:1998: Electromagnetic compatibility (EMC) – Part 2-10: Environment – Description of HEMP environment – Conducted disturbance
IEC 61000-2-11:1999: Electromagnetic compatibility (EMC) – Part 2-11: Environment – Classification of HEMP environments.
IEC 61000-2-13:2005: Electromagnetic compatibility (EMC) – Part 2-13: High-power electromagnetic (HPEM) environments – Radiated and conducted.
IEC 61000-4-23:2016: Electromagnetic compatibility (EMC) – Part 4-23: Testing and measurement techniques – Test methods for protective devices for HEMP and other radiated disturbances.
IEC 61000-4-24:2015: Electromagnetic compatibility (EMC) – Part 4-24: Testing and measurement techniques – Test methods for protective devices for HEMP conducted disturbance.
IEC 61000-4-25:20012001+A1:2012+A2:2019: Electromagnetic compatibility (EMC) – Part 4-25: Testing and measurement techniques – HEMP immunity test methods for equipment and systems.
IEC/TR 61000-4-32:2002: Electromagnetic compatibility (EMC) – Part 4-32: Testing and measurement techniques – High-altitude electromagnetic pulse (HEMP) simulator compendium.
IEC 61000-4-33:2005: Electromagnetic compatibility (EMC) – Part 4-33: Testing and measurement techniques – Measurement methods for high-power transient parameters.
IEC/TR 61000-4-35:2009: Electromagnetic compatibility (EMC) – Part 4-35: Testing and measurement techniques – High power electromagnetic (HPEM) simulator compendium.
IEC 61000-4-36:2020: Electromagnetic compatibility (EMC) – Part 4-36: Testing and measurement techniques – IEMI immunity test methods for equipment and systems.
IEC/TR 61000-5-3:1999: Electromagnetic compatibility (EMC) – Part 5-3: Installation and mitigation guidelines – HEMP protection concepts.
IEC/TS 61000-5-4:1996: Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 4: Immunity to HEMP – Specifications for protective devices against HEMP radiated disturbance.
IEC 61000-5-5:1996: Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 5: Specification of protective devices for HEMP conducted disturbance.
IEC/TR 61000-5-6:2002: Electromagnetic compatibility (EMC) – Part 5-6: Installation and mitigation guidelines – Mitigation of external EM influences.
IEC 61000-5-7:2001: Electromagnetic compatibility (EMC) – Part 5-7: Installation and mitigation guidelines – Degrees of protection by enclosures against electromagnetic disturbances (EM code).
IEC/TS 61000-5-8:2009: Electromagnetic compatibility (EMC) – Part 5-8: Installation and mitigation guidelines – HEMP protection methods for the distributed infrastructure.
IEC/TS 61000-5-9:2009: Electromagnetic compatibility (EMC) – Part 5-9: Installation and mitigation guidelines – System-level susceptibility assessments for HEMP and HPEM.
IEC/TS 61000-5-10:2017: Electromagnetic compatibility (EMC) – Part 5-10: Installation and mitigation guidelines – Guidance on the protection of facilities against HEMP and IEMI.
IEC 61000-6-6:2003: Electromagnetic compatibility (EMC) – Part 6-6: Generic standards – HEMP immunity for indoor equipment.

Veiledere

SINTEF Energiforskning. EMP-sikring av kraftforsyningsanlegg: Håndbok. Lysaker: Energiforsyningens fellesorganisasjon, 2000

Forsvarsbygg. *EMP-handbok: Veiledning i sikring av kritisk infrastruktur mot elektromagnetiske effekter*. Oslo: Forsvarsbygg, 2020. (Distribusjon ved henvendelse til NVE eller Forsvarsbygg)

Beskyttelse av elektroniske installasjoner i totalforsvaret mot elektromagnetisk puls (EMP), retningslinjer fastsatt av Samferdselsdepartementet 24.03.1998

Krysskobling til andre paragrafer og regelverk

§ 7-13 Beskyttelse mot elektromagnetisk puls og interferens

Bokstav j

§ 7-14 j Sikker tidsreferanse setter krav til sikre kilder for tidsangivelse.

Kraftsystemets funksjoner og tilstander kan ha behov for synkronisert tid i driftskontrollsystemet, blant annet for registrering av feil i kraftsystemet og pålitelig drift av datasystemer og kontrollanlegg.

Behovet for nøyaktighet er moderat (~10 ms), så lenge hensikten med systemtiden er begrenset til å synkronisere de ulike komponentene (tjenere, PCer, rutere, brannmurer, dataskjerm mv) i drifts-kontrollsystemet. Behovet øker (~1 ms) når måleverdier og hendelser i kraftsystemet skal ha tidsstempel. Først med instrumentering og digital styring i henhold til IEC 61850 er synkronisering av datastrømmer og enheter et ubetinget krav. Ikke-konvensjonelle instrumenteringsløsninger og dynamisk systemovervåkning med høyoppløste digitale måleverdistrømmer krever eventuelt en nøyaktighet på bedre enn 1 µs.

Den langt vanligste tidskilden i norske kraftforsyningsanlegg og driftskontrollsystemer er direkte synkronisering ved bruk av GPS-mottakere. Spesielt relevant er derfor å redusere sårbarheten ved tap av GPS-signal.

Også atmosfæriske forhold kan forårsake tap eller degradering av GPS-signaler over et større geografisk område.

GPS-mottakere med integritetsfunksjon gjør bruk av informasjon fra flest mulig satellitter for å vurdere gyldigheten av signalene. GPS-mottakere uten integritetsfunksjon er sårbare for støysendinger, og kan vanskelig skille mellom ekte og falske GPS-signaler.

Radiointerferens kan være utilsiktet eller tilsiktet. Ved mistanke om utilsiktet radiointerferens, må den nasjonale frekvensmyndigheten (NKOM) https://www.nkom.no/ kontaktes, slik at kilden kan avdekkes og fjernes.

Selv om driftskontrollsystemet hos en KBO-enhet ikke er avhengig av nøyaktig tid, så vil bortfall eller feilvisning av tid få driftsmessige konsekvenser. KBO-enheten bør derfor vurdere risiko og eventuelt treffe passende tiltak.

De GPS-mottakerne som er mest utbredt i kraftforsyningen, leveres med kvartsklokker, og er utstyrt med kun enkle antenner og har få muligheter for konfigurering. KBO-enhetene bør vurdere om de vanligste mottakerne er tilstrekkelig sikre og nøyaktige.

Mulige tiltak er å:

- Utstyre GPS-mottakerne med bedre antenner som gir større signal/støy-forhold. Dermed vil GPS-mottakerne bli mer resistente mot støysendinger og andre forstyrrelser av signalmottaket, herunder romvær og atmosfæriske forstyrrelser
- Konfigurere stasjonære GPS-mottakere med sin sanne posisjon, og sørge for alarm når posisjonsestimatet havner utenfor unøyaktighetsrommet
- Installere redundante mottakere, fordelt på GPS og Galileo. En viktig faktor er at GPS og Galileo benytter ulike frekvenser
- Samle inn og overvåke navigasjonsmeldingene som GPS-mottakerne behandler. Dermed kan eventuelle falske kodestrømmer avdekkes, og alarm gis
- Utstyre GPS-mottakerne med mer nøyaktige klokker slik at utfall av GPS-signaler kan tolereres over lengre tidsrom
- Andre klokker, for eksempel atom-ur

Standarder
IEC 61850-9-2:2011+A1:2020: Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3
IEC TR 61850-90-4:2013: Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines
IEC/IEEE 61850-9-3:2016: Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation

Veiledere
Norsk Romsenter, Vurdering av sårbarhet ved bruk av globale satelittnavigasjonssystemer i kritisk infrastruktur, Oslo, mars 2013.

Bokstav k

§ 7-14 k: Krav til leverandører

Her settes krav til hvilke leverandører som får levere systemer til norsk kraftforsyning. Kravet gjelder komplette leveranser til driftskontrollsystemet, og ikke enkeltstående komponenter som utgjør en del av en helhet. Store globale leverandører har produksjon og forskning lokalisert i ulike deler av verden, og de er avhengige av leverandører og underleverandører. Å utelukke enkeltkomponenter er derfor ikke gjennomførbart i praksis. En sikker kraftforsyning inngår i NATOs sju basiskrav til vertsnasjoner som mottar NATO-støtte. Når det gjelder anskaffelse av driftskontrollsystemer er anskaffelse foretatt nært opp til sikkerhetslovens krav derfor å foretrekke. For virksomheter som ikke er underlagt sikkerhetsloven, vil dette kravet sammen med § 6-6 Begrenset anbudsinnbydelse gi virksomhetene noen verktøy. For ordens skyld presiserer vi at bestemmelsen ikke er ment å utelukke norske leverandører.

7.15 Særskilte krav til driftskontrollsystem klasse 3

§

§ 7-15.Særskilte krav til driftskontrollsystem klasse 3
Foruten de generelle kravene samt særskilte krav til beskyttelse av driftskontrollsystem i klasse 2, skal virksomheter med driftskontrollsystem i klasse 3 oppfylle følgende tilleggskrav:

a. ***Reserve driftssentral***
Virksomheter skal ha reserve driftssentral som skal plasseres i sikker avstand til ordinær driftssentral, slik at ikke samme hendelse kan ramme begge.

Reserve driftssentral skal til enhver tid være klar til bruk og være utstyrt slik at den kan fungere helt uavhengig av ordinær driftssentral og kunne ivareta alle driftskontrollfunksjoner.

Virksomheter skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptrapping av bemanning, jf. § 7-9, annet ledd.

b. ***Bemanning av driftssentral***
Driftssentralen skal være døgnbemannet.

Opptrapping av bemanningen skal kunne skje innen én time etter at påkalling er gjort.

Virksomheten skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptrapping av bemanning, jf. § 7-9, andre ledd.

c. ***Ekstern tilkobling til driftskontrollsystemet***
Kobling i nettanlegg eller styring av øvrige anlegg gjennom ekstern tilkobling er ikke tillatt.

d. ***Systemredundans***
Sambandsveiene i driftskontrollsystemet skal utføres så sikre og robuste og med en slik redundans og avstand at ikke samtidige eller påfølgende hendelser som uvær, brann eller omfattende teknisk svikt hindrer eller skader begge føringsveier og andre redundante delsystem.

Frem til alle anlegg i klasse 3 skal virksomheten ha kontroll og råderett over alle komponenter og andre tekniske løsninger i minst én sambandsvei, og beskytte disse, jf. kapittel 5.

e. ***Beskyttelse mot EMP og EMI***
Det skal gjennomføres sikringstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 3 som driftskontrollsystemet styrer. Beredskapsmyndigheten kan i særskilte tilfeller godkjenne beredskapstiltak som alternativ til sikringstiltak.

I sambandsvei til anlegg i klasse 2 som driftskontrollsystemet styrer, skal det gjennomføres sikrings- eller beredskapstiltak.

f. Fastsettelse av særlige krav til bemanning
For spesielt viktige driftskontrollsystemer kan beredskapsmyndigheten fastsette særlige krav, også til bemanning, jf. § 5-7.

Hvordan oppfylle kravet

Kravene i § 7-15 er detaljerte tilleggskrav til klasse 3 driftskontrollsystemer. Disse kravene kommer i tillegg til grunnkrav som er oppstilt tidligere i kapittel 7 i forskriften og krav som er stilt til klasse 2 driftskontrollsystemer i § 7-14.

Bokstav a

§ 7-15.a. Reserve driftssentral stiller krav til en operativ fysisk reservedriftssentral som virksomheten kan ta i bruk på kort varsel. Den skal plasseres i så lang avstand at samme hendelse ikke rammer begge sentralene. Med hendelser mener NVE ekstraordinære hendelser, se ellers § 2-5 for eksempel på hendelser. Sentralen må derfor ha egnet utstyr og tilstrekkelig bemanning i tillegg til egen fysisk lokasjon. Redundanskravet til servere, front-end og samband kan oppfylles ved at ett system er plassert på samme sted som driftssentralen, og det andre systemet der reservedriftssentralen er plassert.

Bokstav b

§ 7-15b. Bemanning av driftssentral stiller krav til kapasitet (døgnbemannet) og å være operativ med økt kapasitet innen en time. Bemanningsbehovet skal vurderes minimum årlig.

Bokstav c

§ 7-15c. Ekstern tilkobling til driftskontrollsystemet setter et tydelig forbud mot å kople eller styre øvrige anlegg gjennom ekstern tilkopling utenom driftssentralen. Det er forbud mot å styre nett og prosesser hjemmefra.

Bokstav d

§ 7-15d. Systemredundans skjerper ytterligere kravene til redundans i sambandsveiene i driftskontrollsystemet, både med hensyn til innbyrdes separasjon av sambandsveier og med hensyn til at virksomheten selv skal ha kontroll over minst én sambandsvei som også er sikret iht kravene i kapittel 5.

Bokstav e

§ 7-15 e. Beskyttelse mot EMP/EMI setter krav til EMI/EMP-sikringstiltak, og bygger videre på § 7-13 og § 7-14i.

Tilleggskrav til klasse 3 driftskontrollsystem (Merk! Kravene til klasse 2 gjelder også)

Grunn-krav	Tilleggskrav klasse 2 og 3 § 7-14	Ytterligere tillegg for klasse 3 § 7-15
§ 7-1	Foruten de generelle krav til beskyttelse av driftskontrollsystemet, skal virksomheter med driftskontrollsystem i klasse 2 oppfylle følgende tilleggskrav:	Foruten de generelle kravene samt særskilte krav til beskyttelse av driftskontrollsystem i klasse 2, skal virksomheter med driftskontrollsystem i klasse 3 oppfylle følgende tilleggskrav:
§7-8	a. *Sikkerhetskopier* Virksomheten skal jevnlig teste at gjenoppretting av elektroniske	

	sikkerhetskopier fungerer etter hensikten.	
§ 7-2	b. *Sikkerhetsrevisjon* Virksomheten skal jevnlig gjennomføre en sikkerhetsrevisjon og kontroll av pålagte beskyttelsestiltak i driftskontrollsystemet. Revisjonens formål skal være å påse at tiltakene faktisk er etablert og fungerer etter sin hensikt.	
§ 7-4	c. *Overvåking og logging* Virksomheten skal ha automatisk overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i driftskontrollsystemet.	
§ 7-8	d. *Utilgjengelig driftssentral* Dersom driftssentralen blir utilgjengelig, skal virksomheten kunne betjene og manuelt styre anlegg som inngår i virksomhetens driftskontrollsystem. I tillegg skal virksomheten ha planer for alternativ drift dersom driftssentralen blir utilgjengelig over lengre tid.	a. *Reserve driftssentral* Virksomheter skal ha reserve driftssentral som skal plasseres i sikker avstand til ordinær driftssentral, slik at ikke samme hendelse kan ramme begge. Reserve driftssentral skal til enhver tid være klar til bruk og være utstyrt slik at den kan fungere helt uavhengig av ordinær driftssentral og kunne ivareta alle driftskontrollfunksjoner. Virksomheter skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptrapping av bemanning, jf. § 7-9, annet ledd.
§ 7-9	e. *Bemanning av driftssentral* Virksomheten skal sørge for at alle påregnelige ekstraordinære situasjoner eller hendelser i energisystemet eller i driftskontrollsystemet umiddelbart oppdages og håndteres uten unødig opphold. Virksomheten skal senest innen én time kunne bemanne driftssentralen. Virksomheten skal ha en vaktordning som til enhver tid sikrer rask opptrapping av bemanningen ved behov.	b. *Bemanning av driftssentral* Driftssentralen skal være døgnbemannet. Opptrapping av bemanningen skal kunne skje innen én time etter at påkalling er gjort. Virksomheten skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptrapping av bemanning, jf. § 7-9, andre ledd. f. *Fastsettelse av særlige krav til bemanning* For spesielt viktige driftskontrollsystemer kan beredskapsmyndigheten fastsette særlige krav, også til bemanning, jf. § 5-7.
§ 7-10	f. *Ekstern tilkobling til driftskontrollsystemet*	c. *Ekstern tilkobling til driftskontrollsystemet*

	Ved tilkobling fra leverandører skal driftssentralen være bemannet. Virksomheter skal ha kontrollordning for korrekt verifisering av de brukere som er godkjent til å benytte ekstern tilkobling for tilgang til driftskontrollsystemet. Det er ikke tillatt at én brukeridentitet deles mellom flere personer eller systemer. Virksomheter skal sørge for at ekstern tilkobling utføres fra et sted med tilstrekkelig sikre omgivelser. Virksomheter skal utarbeide interne regler for hva som er et sikkert sted. Den eksterne tilkoblingen skal kun åpnes når det er behov for å få tilgang til driftskontrollsystemet. Tilkoblingen skal være lukket når den ikke er i bruk. Det skal foreligge en egen skriftlig prosedyre for ekstern tilkobling. Dersom KBO-enheten kan foreta styring av anlegg i kraftforsyningen gjennom ekstern tilkobling, skal styringen kun skje etter tillatelse eller retningslinjer fra bemyndiget person. Enhver påkobling til driftskontrollsystemet gjennom ekstern tilkobling skal loggføres.	Kobling i nettanlegg eller styring av øvrige anlegg gjennom ekstern tilkobling er ikke tillatt.
§ 7-11	g. *Systemredundans* Samband i driftskontrollsystemet skal fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett. Driftskontrollsystemet frem til anlegg i klasse 2 og 3 skal være redundant frem til det lokale kontrollanlegget. I det lokale kontrollanlegget skal virksomheten vurdere behovet for redundans. Redundante føringsveier for samband og redundante komponenter i driftskontrollsystemet skal være fysisk adskilte og uavhengige slik at én enkelt feil eller hendelse ikke medfører tap av viktige funksjoner. Det skal etableres reparasjonsberedskap for alt samband, jf. kapittel 4 og § 7-8.	d. *Systemredundans* Sambandsveiene i driftskontrollsystemet skal utføres så sikre og robuste og med en slik redundans og avstand at ikke samtidige eller påfølgende hendelser som uvær, brann eller omfattende teknisk svikt hindrer eller skader begge føringsveier og andre redundante delsystem. Frem til alle anlegg i klasse 3 skal virksomheten ha kontroll og råderett over alle komponenter og andre tekniske løsninger i minst én sambandsvei, og beskytte disse, jf. kapittel 5.
§ 7-10	h. *Særskilt om dublering* Ved dublering som benytter identiske teknologier og løsninger i driftskontrollsystemet, må virksomheten innrette seg slik at	

	samme systemfeil ikke rammer alle dublerte system samtidig	
§ 7-13	i. *Beskyttelse mot EMP og EMI* Det skal gjennomføres sikrings- eller beredskapstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 2 og 3 som driftskontrollsystemet styrer.	e. *Beskyttelse mot EMP og EMI* Det skal gjennomføres sikringstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 3 som driftskontrollsystemet styrer. Beredskapsmyndigheten kan i særskilte tilfeller godkjenne beredskapstiltak som alternativ til sikringstiltak. I sambandsvei til anlegg i klasse 2 som driftskontrollsystemet styrer, skal det gjennomføres sikrings- eller beredskapstiltak.
	j. *Sikker tidsreferanse* Driftskontrollsystem som er avhengig av eksakt tidsreferanse, skal ha sikre kilder for tidsangivelse.	
	k. *Krav til leverandører* For leveranser til driftskontrollsystemer tillates kun utenlandske leverandører fra land som er medlem i EFTA, EU eller NATO. En leveranse omfatter levering av utstyr, komponenter, programvare, data, programmeringstjenester, oppdateringer, feilretting, service og vedlikehold.	

7.16 Vern av kraftsystem i regional- og transmisjonsnett

§

§ 7-16.Vern av kraftsystem i regional- og transmisjonsnett
Kommunikasjonsbaserte vernsystemer i transmisjons- og regionalnett skal ha pålitelige og sikre samband som fungerer upåvirket av feiltilstander i kraftsystemet, og sørger for overføring av nødvendige signaler og meldinger mot relevante driftssentraler.

Vernsystemer skal sørge for rask og selektiv frakopling av enhet med funksjonsfeil for å begrense konsekvensen av feil i kraftsystemet.

Hvordan oppfylle kravet?

Vernsystemet kan være en del av driftskontrollsystemet, eller bruke de samme kommunikasjons-veiene. § 7-16 inneholder ikke krav om at det skal etableres vern, kun om sikkerheten i vern-kommunikasjonen og at feil skal frakobles raskt og selektivt. Bestemmelser i kapittel 7 gjelder for vernsystemene med utgangspunkt i driftskontrollsystemets eller lokalkontrollsystemets klasse.

Bestemmelsen stiller krav til sikring av elektronisk kommunikasjon i viktige vernsystemer, herunder fjerninnstilling av vern, og at vernsystemet skal ha innebygde egenskaper som begrenser konsekvensene av feil i vernet.

Kommunikasjonen innbyrdes mellom vern, og mellom en servicetekniker eller applikasjon som skal fjern-innstille vern, må være sikret mot ikke godkjent tilgang og ikke godkjent endring.

I forskriftsbestemmelsene til systemansvarsforskriften og forskrift om elektriske forsyningsanlegg er det krav om å ha fungerende vernsystemer.

I Statnetts veiledning NVF 2020 finnes detaljerte bestemmelser om vernfunksjonalitet med tilhørende krav.

Veiledere

Statnett NVF 2020 Nasjonal veileder for funksjonskrav i kraftsystemet
DSB Forskrift om elektriske forsyningsanlegg (FEF)

Krysskobling til andre paragrafer og regelverk

Systemansvarsforskriften § 20. *Vern og reléplanlegging* og i § 21. *Systemvern*.
FEF § 2-11. *Overvåking og kontrollsystemer*
FEF § 4-10. *Vern, kontroll og hjelpesystemer*

§ 7-10.Ekstern tilkobling til driftskontrollsystem
§ 7-11.Systemredundans i driftskontrollsystemet
§ 7-13.Beskyttelse mot elektromagnetisk puls og interferens
§ 7-14.Særskilte krav til driftskontrollsystem klasse 2
§ 7-15.Særskilte krav til driftskontrollsystem klasse 3

7.17 Mobile radionett – driftsradio

§

§ 7-17. Mobile radionett - driftsradio
KBO-enheter som er avhengig av pålitelig mobilkommunikasjon for drift, sikkerhet eller gjenoppretting av funksjon, skal ha tilgang til et mobilt sambandssystem. Dette sambandssystemet skal:

a. Omfattes av den generelle sikringsplikten etter § 5-1
b. Til enhver tid holdes i funksjonsdyktig stand, være klar til bruk, og det skal være rask tilgang på kritiske reservedeler og kompetanse på feilretting
c. Kunne betjenes av personell med nødvendig kompetanse til bruk
d. Ha tilstrekkelig dekningsgrad for kraftforsyningens anlegg og drift
e. Kunne fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett
f. Ha tilstrekkelig nødstrøm ved omfattende eller langvarige strømbrudd, herunder et nødstrømssystem med automatisk start og minimum 48 timer selvstendig driftstid
g. Ha nødvendig funksjonalitet med blant annet direkte apparat til apparat-kommunikasjon, gruppesending og felles oppkall
h. Kunne fungere som reservesamband om annet viktig samband svikter
i. Der hvor radionettet benytter anlegg tilhørende et klassifisert driftskontrollsystem eller hvor det må regnes som en del av dette, skal sambandssystemet beskyttes i henhold til driftskontrollsystemets klasse
j. Der hvor radionettet er digitalisert og f.eks. baserer seg på IP-løsninger, skal dette sikres mot uautorisert tilgang, spredning av uønsket programvare, urettmessig overtakelse m.m. etter relevante bestemmelser i denne forskrift

Hvordan oppfylle kravet

Hensikten med bestemmelsen er å sikre at de virksomhetene som er avhengige av et mobilt radionett, anskaffer et system som også fungerer i ekstraordinære situasjoner, for eksempel der forsyning av elektrisitet til et område faller ut.

Bestemmelsen om mobilt radionett er teknologinøytral. NVE setter ingen begrensninger for valg av system eller teknologi så lenge kravene i bestemmelsen og andre relevante krav i denne forskriften er oppfylt.

KBO-enheten må sikre uavhengighet i forhold til funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett. Nødstrøm for 3 døgns drift er et tiltak som kan bidra til det. Dersom tjenesten driftsradio kjøpes fra ekstern leverandør, må tjenesten ved strømavbrudd og brudd til sentral server hos leverandør tilby kommunikasjon i form av minimum talesamband mellom KBO-enhetens mannskap på anlegg ute og driftssentralen i minimum 48 timer.

Driftsradioen må ha tilstrekkelig geografisk dekningsgrad. Det betyr at mannskap hos KBO-enheten må kunne kommunisere med driftssentralen og utføre arbeid på alle viktige elkraftanlegg som KBO-enheten har ansvar for. KBO-enheten må ha oversikt over hvilke anlegg som er viktige for å opprettholde forsyningssikkerhet. Dersom det ikke er dekning på stedet der mindre viktige anlegg står,

må det være mulig å forflytte seg til et dekningsområde innenfor rimelig tid. Hva som er rimelig tid, avgjøres av KBO-enheten.

Systemet må som et minimum gi tilgang til talekommunikasjon mellom KBO-enhetens mannskap ute og driftssentralen selv om det offentlig ekom-nettet svikter. Risiko for svikt i radionettet reduseres ved å sikre at radionettet har tilstrekkelig nødstrøm for minimum 48 timer i områder der viktige elkraftanlegg er lokalisert. Dersom tjenesten kjøpes eksternt av leverandør, må virksomheten undersøke hvilke tjenester eller dekningsområde i radionettet som faller ut dersom driftsradioen mister kontakt med sentral server hos leverandøren, eller dersom offentlig ekom-nett faller ut. KBO-enheten må avhengig av konsekvensene, iverksette kompenserende tiltak.

Mobilt radionett blir normalt ikke klassifisert og er som sådan ikke en del av et klassifisert driftskontrollsystem, da det nødvendigvis ikke er sammenheng mellom driftskontrollsystemets betydning og radionettets betydning. Dersom KBO-enheten likevel, i tillegg til talekommunikasjon, benytter radiosystemet til overføring av signaler til driftskontrollsystemet eller andre viktige signaler, må KBO-enheten i tillegg oppfylle relevante krav til beskyttelse av driftskontrollsystemet i henhold til bestemmelsene. Dette gjelder særlig krav til redundans, særskilte krav til fysisk beskyttelse, EMP og EMI samt beskyttelse mot IKT-trusler. KBO-enheten bør også vurdere redundans ved for eksempel å ha to overføringsmuligheter i viktige dekningsområder, uavhengig om man benytter radiosystemet til andre formål enn talesamband. NVE anser ringstruktur av basestasjoner som et akseptabelt redundanstiltak.

Sjekkliste for mobil driftsradio

Strømforsyning og kabling
Ordinær strømforsyning, nødstrøm og samband bør føres inn i bygninger gjennom jordkabler. Stasjonens kabling bør organiseres slik at den beskytter mot overspenninger. Sikringsskap og liknende plasseres innendørs. Likerettere bør dupliseres og overvåkes med alarmer. Stasjonene bør utstyres med batterianlegg med driftstid på minst 72 timer. Alternativt kan stasjonen ha batterianlegg med driftstid på minst 48 timer dersom stasjonært nødstrømsaggregat er installert. Krav til nødstrøm kan reduseres dersom man har god adkomst til stasjonen.

Fysiske sikringstiltak

- Viktige og utsatte stasjoner bør bygges i betong, eventuelt stålkontainer (dette gir bl.a. beskyttelse mot brann, innbrudd og hærverk)
- Viktige komponenter bør plasseres i avlåste rom uten vinduer, med innbruddsalarm til døgnbemannet sentral (eventuelt hjemmevakt)
- Vinduer bør tildekkes med solide lemmer, låst eller boltet til innsiden
- Kabelføringer til mast bør føres i tildekket kanal eller i kabelbro slik at de ikke er lett tilgjengelige for uvedkommende
- Jordkabler bør beskyttes mekanisk ved at de legges i egne rør eller betongkanaler
- Antenner og master er vanskelige å beskytte. Her bør det anskaffes reserveutstyr og også tilrettelegge for alternative føringsveier for kommunikasjon. Master bør beskyttes med klatrehindre
- ARom som inneholder elektronisk utstyr og som har betydning for driften av driftsradiostasjonen (datarom og liknende), skal gjennom en risikovurdering vurderes skjermet mot EMP/EMI, jf § 7-13. *Beskyttelse mot elektromagnetisk puls og interferens*

Beskyttelse av digitale sambandsløsninger
Digitale driftsradioløsninger er utsatt for samme type trusler som annen IKT. Kravene i kapittel 6 og i kapittel 7 gjelder dersom radiosystemet også benyttes til signalering i driftskontrollsystemet.

Reservedeler og reparasjonsberedskap
Virksomhetens beredskapsplan må inkludere reparasjon av driftsradioanlegg. Virksomheten bør ha de mest kritiske komponentene i radiosystemet på lager. Der det benyttes viktige enheter med svært lang leveringstid, bør leverandøren kontaktes for å inngå avtale om lagerhold. Egne medarbeidere bør ha tilstrekkelig kompetanse for enkel feilsøking og -retting. Behov for assistanse må avtales med leverandør eller andre.

Krav til kompetanse for å installere utstyr i radioanlegg er regulert i lov om elektronisk kommunikasjon kommunikasjon (ekomloven) § 2-14, med tilhørende forskrifter; forskrift om elektroniske kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) kapittel 9, samt forskrift om autorisasjon for installatør av elektronisk kommunikasjonsnett og radioutstyr (autorisasjonsforskriften) kapittel 9.

Lov om elektronisk kommunikasjon (Ekomloven)

Forskrift om autorisasjon for virksomhet som utfører installasjon og vedlikehold av elektronisk kommunikasjonsnett (autorisasjonsforskriften)

Maler

Standarder

Veiledere

Krysskobling til andre paragrafer og regelverk
§ 2-10 Internkontroll
§ 4-7 Samband
§ 5-1 Sikringsplikt
Vedlegg til kap 5
Kapittel 6
Kapittel 7 dersom driftsradioen benyttes til driftskontrollfunksjoner
Enkeltvedtak Vedtak om beredskapsmessige kommunikasjonsmidler (2015, Unntatt offentlighet)
EKOM-loven § 2-14
Ekom-forskriften kapittel 9
Autorisasjonsforskriften kapittel 9